5. Auflage



Tails

The amnesic incognito live system

Anleitung zur Nutzung des Tails-Live-Betriebssystems für sichere Kommunikation, Recherche, Bearbeitung und Veröffentlichung sensibler Dokumente

Hefte zur Förderung des Widerstands gegen den digitalen Zugriff

Band I: Tails – The amnesic incognito live system

capulcu productions 5. überarbeitete Auflage | Oktober 2017

V.i.S.d.P. E. Schmidt | Am Zuckerberg 14 | 21984 Silikontal

Anleitung zur Nutzung des Tails-Live-Betriebssystems für sichere Kommunikation, Recherche, Bearbeitung und Veröffentlichung sensibler Dokumente

Eine digitale Version dieser Anleitung sowie redaktionell bearbeitete Anmerkungen, Änderungen und Neuerungen findet ihr unter **https://capulcu.blackblogs.org** . Die Verbindung zur Webseite erfolgt verschlüsselt. Um zu überprüfen, dass ihr wirklich auf unserer Seite gelandet seid, drucken wir hier eine *Prüfsumme* unseres Webseiten-Zertifikats ab (gültig bis 6.1.2018):

sha256: `A2:D4:51:8E:DB:90:A3:A1:5F:A2:0B:03:88:DD:91:84:`
`20:0A:59:CD:8A:BE:45:30:FD:05:2E:EB:3D:D5:96:E6`

Wir freuen uns über Feedback. Den *Schlüssel* zu unserer Mail-Adresse findet ihr auf unserer Webseite **https://capulcu.blackblogs.org** . Wir drucken hier zur Überprüfung der Echtheit den *Fingerprint* dieses Schlüssels ab:
capulcu@nadir.org AF52 0854 7EF1 711A F250 57CB D0D0 A3C5 DF30 9590

Tails ist zur Überprüfung der Echtheit des Downloads ebenfalls mit einem Schlüssel signiert. Den Schlüssel der Tails-Entwickler*innen findet ihr auf der Seite **https://tails.boum.org.** Wir drucken hier den zugehörigen Fingerprint ab:
tails@boum.org A490 D0F4 D311 A415 3E2B B7CA DBB8 02B2 58AC D84F

Inhalt

Einführung

Repressionsorgane interessieren sich seit einiger Zeit verstärkt für das „Digitale“. Hausdurchsuchungen bedeuten eigentlich immer, das alles, was nach Rechner, Smartphone, Datenträger jeder Art etc. aussieht, danach beschlagnahmt ist. An einigen Grenzen (z.B. der USA) kommt es vor, dass der/die Grenzer*in nach dem Passwort für Accounts in sozialen Netzen fragt. Diverse Armeen dieser Welt überschlagen sich beim Aufstellen von „Cyberwar“-Einheiten. Spätestens seit den Veröffentlichungen von Edward Snowden ist bekannt, dass die Geheimdienste NSA und GCHQ in großem Umfang Daten aus dem Netz saugen - wenn es geht, dann sogar automatisiert, bis hin zum massenweisen „Hacken“ von Rechnern[1].

Wir empfehlen angesichts dieser Situation, den Kopf nicht in den Sand zu stecken, sondern die vorhandenen technischen Möglichkeiten zum Selbstschutz voll auszuschöpfen. Tails ist ein großer Schritt in diese Richtung. Das Live-Betriebssystem ist ein eigenständiges Betriebssystem, was von DVD oder USB-Stick gestartet werden kann, ohne es zu installieren. Euer Standard-Betriebssystem auf der Festplatte wird nicht angefasst.

Tails hilft bei der Bearbeitung von sensiblen Text-, Grafik- und Tondokumenten. Tails verwendet beim Surfen, Mailen und Chatten automatisch die Anonymisierungssoftware „*Tor*“. Tails erschwert die Wiedererkennbarkeit eures Rechners im Netz durch die Änderung der „MAC-Adresse“. Was das ist und wozu das von Nutzen ist, erklärt die Einführung dieser Anleitung.

Tails hinterlässt bei richtiger Nutzung keine Spuren auf dem Rechner - die Festplatte bleibt unberührt. Ein eventuell (auf Betriebsystemebene) eingeschleuster Schadcode kann sich auf einer Live-DVD oder einem schreibgeschützten Live-USB-Stick[2] als Start-Medium nicht „festsetzen“ und euch beim nächsten Rechnerstart nicht mehr behelligen. Tails ist allerdings Software, gegen eine manipulierte Hardware kann es nicht schützen - höchsten warnen.

Konkrete Blockade digital-totalitärer Erfassung

Wer sich gegen die Verletzung von Persönlichkeitsrechten durch das Ausspionieren jeglicher Netzdaten, gegen DNA-Datenbanken und (Drohnen-)Kameraüberwachung politisch aktiv zur Wehr setzt, sollte auch bei der Preisgabe seiner Alltagsdaten nicht nur sparsamer, sondern vor allem strategisch (und damit ganz anders als erwartet) vorgehen.

Insbesondere das Zusammenführen unserer verschiedenen Aktivitäten, Interessen, Neigungen, Einkäufe, Kommunikationspartner*innen, (...) zu einer integralen „Identität“ ist die Grundlage für die Mächtigkeit von schnüffelnden Analysewerkzeugen - egal, ob sie ökonomisch-manipulativen oder repressiven Absichten entspringen. Tails hilft Nicht-Expert*innen, mit annehmbarem Aufwand dieses „integrale Ich“ auf unterschiedliche digitale Identitäten zu verteilen. Noch besser: Ihr nutzt mit mehreren vertrauenswürdigen Personen einen gemeinsamen Mail-, Chat-, Blog-, oder Forum-Account orts-anonymisierend. Auch das erledigt Tails über die Anonymisierungssoftware *Tor*.

Zur (Wieder-)Erlangung eines Mindestmaßes an Privatheit und Daten-Souveränität raten wir darüber hinaus zur Verschlüsselung aller Inhalte, zum lokalen Speichern eurer Daten (ohne Cloud), zur Facebook-Verweigerung, zur gezielten Drosselung der Teilhabe am digitalen Dauersenden (das möglichst „unsmarte“[3] ! Mobiltelefon so oft es geht zu Hause lassen) und zum Offline-Einkauf mit Barzahlung. Im Netz möglichst wenig Spuren zu hinterlassen muss zu einer Selbstverständlichkeit und Grundfertigkeit werden. *Tor* ist zur Zeit das beste Werkzeug dafür, das es gibt, und Tails hilft uns (unter anderem), bei der Nutzung von *Tor* möglichst wenig Fehler zu machen.

Verglichen mit dem, was wir an Selbstbestimmtheit bereits verloren haben, ist der Aufwand für ein abgeändertes Alltagsverhalten minimal, auch wenn es vielen von uns „unbequem“ erscheint. Die „bequeme“ Alternative hingegen bedeutet Kontrollierbarkeit, Vorhersagbarkeit, Manipulierbarkeit und erhöhtes Repressions-Risiko – nicht nur für euch, sondern auch für diejenigen, mit denen ihr kommuniziert.

Wozu ein Live-Betriebssystem (auf DVD oder USB-Stick) ?

Die wichtigsten Gründe für die Verwendung eines Live-Betriebssystems wie Tails sind dessen Vergesslichkeit und Unveränderbarkeit.

Nach dem Herunterfahren des Rechners sind alle Daten, die ihr zuvor nicht explizit auf einen (externen) Datenträger gesichert habt, wieder weg. Der ohnehin vergessliche Arbeitsspeicher eures Rechners wird beim Herunterfahren zusätzlich mit Zufallszahlen überschrieben und die Festplatte bleibt von der Tails-Sitzung unberührt[4].

1 The Intercept, Glenn Greenwald, Ryan Gallagher, 12.3.2014 https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/

2 USB-Sticks mit mechanischem Schreibschutzschalter sind leider nur selten im Offline-Handel erhältlich. Hersteller solcher Sticks ist u.a. die Firma *Trekstore*.

3 Ein Mobiltelefon ohne WLAN und Bluetooth ist ein besserer Schutz.

4 Es sei denn, ihr speichert explizit einzelne Dateien auf die interne Festplatte. Davon raten wir ab!

Keine Systemdateien, die verraten, welche USB-Sticks ihr benutzt habt, keine versteckten Rückstände eurer Internetrecherche, kein Hinweis auf „zuletzt bearbeitete“ Dokumente, keine Überbleibsel einer Bildbearbeitung und vor allem auch keine Schad-/Schnüffelsoftware, die sich während eurer Sitzung irgendwo in den Betriebssystemdateien eingenistet haben könnte – alles weg nach Abschluss eurer Arbeit. Euer „normales“ Betriebssystem (auf der Festplatte) dieses Rechners bleibt unverändert. Der Rechner trägt auch keine Spur, die darauf hindeutet, dass es diese Tails-Sitzung gegeben hat.

Um bei sensibler Arbeit wirklich sicher zu gehen, dass tatsächlich nichts zurückbleibt, sollte sich Tails entweder auf einem unveränderlichen Datenträger befinden (z.B. einer gebrannten DVD oder einem USB-Stick mit mechanischem Schreibschutzschalter), oder aber (per Startoption toram[5]) vollständig in den Arbeitsspeicher des Rechners geladen werden. Dann könnt ihr nämlich den Datenträger, auf dem sich Tails befindet, nach dem Hochfahren des Rechners noch vor Arbeitsbeginn auswerfen/abziehen.

Vorteile bei der Nutzung von Tails

Bei Tails werden zudem alle Netzwerkverbindungen nach „draußen“ über eine fertig konfigurierte *Tor*-Software geleitet[6]. Das heißt, ihr habt weniger Möglichkeiten, eure Identität versehentlich doch preiszugeben. Selbstverständlich müsst ihr auch mit Tails wichtige Grundlagen für die *Tor*-Nutzung[7] wie z.B. den Unterschied zwischen Verschleierung der Identität und Verschlüsselung der Verbindung berücksichtigen. Aber dazu später mehr. Tails hat darüber hinaus viele sicherheitsrelevante Softwarepakete integriert und wird kontinuierlich gepflegt. Ihr dürft etwa alle zwei Monate mit einer neuen Tails-Version rechnen.

Tails basiert auf der Linuxdistribution Debian und ist keine selbstentworfenes System. Sicherheitsupdates und die Weiterentwicklung der ganzen Software wird größtenteils von Debian übernommen. Es ist erklärter Anspruch der Tailsentwickler*innen, immer nahe an Debian dran zu bleiben und die Modifikationen auf das Nötige zu beschränken. Das hat den netten Nebeneffekt, dass bei Fragen zur Software die Dokumentation von Debian (oder dem ebenfalls debianbasierten Ubuntu) in vielen Fällen auch weiterhilft. Tails besteht also zum großen Teil aus bekannter Software, die nur anders konfiguriert wurde - wenn überhaupt.

Da Tails mittlerweile ein sehr umfangreiches und vielseitig einsetzbares Live-System ist und die (derzeit nur in englischer und französischer Sprache vollständige) Dokumentation auf der Webseite https://tails.boum.org entsprechend reichhaltig ist, versuchen wir hiermit eine verdichtete, aber trotzdem verständliche Einführung für Computer-Nicht-Expert*innen zur Verfügung zu stellen.

Wir werden im Folgenden drei Nutzungsmodelle für Tails beschreiben:

a) Tails als System für sensible Arbeiten auf einem Rechner mit Internetzugang

Hier lernt ihr den Umgang mit den von Tails zur Verfügung gestellten Programmen. Die Verbindung zum Netz erledigt ein weitgehend automatisierter und einfach zu bedienender Netzwerk-Manager. Die Oberfläche sieht sehr ähnlich aus wie bei eurem normalen Betriebssystem auf der Festplatte - egal ob ihr Windows, Mac-OS X oder ein Linux-Betriebssystem nutzt, ihr werdet euch bei Tails schnell zurecht finden.

b) Tails als „Quasi-Schreibmaschine“ für hoch-sensible Arbeiten auf einem völlig abgeschotteten Rechner ohne Netz, bei dem Festplatte(n), WLAN- und Bluetooth-Adapter ausgebaut sind.

Hier lernt ihr den Umgang mit besonders sensiblen Dokumenten. Das kann die Bearbeitung von Texten, Fotos, Tonaufnahmen oder die Erstellung ganzer Bücher sein. Hier darf nichts schief gehen. Deshalb raten wir in solchen Fällen zu einem Rechner mit beschränkten Fähigkeiten *(keine Festplatte, keine Internetverbindung, kein WLAN, kein Bluetooth)*, der euch zudem nicht persönlich zugeordnet werden kann.

c) Persistenz: Tails als Reise- und Alltagssystem

In Erweiterung zur ersten Auflage dieses Heftes haben wir uns entschlossen, eine weitere Nutzungsmöglichkeit von Tails zu dokumentieren: Tails auf einem USB-Stick mit einer zusätzlichen (verschlüsselten) Daten-Partition[8], auf der Einstellungen, Mails oder andere Daten dauerhaft gespeichert bleiben. In dieser Nutzungsart ist der Tails-Stick nicht mehr *unveränderbar*[9] und Tails nicht mehr vollständig *vergesslich*.

Im Vergleich zu a) und b) ist diese Nutzung also explizit unsicherer! Im Vergleich zu eurem Alltagsrechner auf der Festplatte aber in der Regel viel sicherer, denn Tails lenkt weiterhin jede Kommunikation mit der Außenwelt sicher durch das Anonymisierungsnetz *Tor*. Wer also einen Reiselaptop mit Netzzugang nutzt, aber z.B. seinen Aufenthaltsort beim Mailen und Chatten nicht verraten will, und dennoch bequemen Zugriff auf seine bisherigen Mails und Dokumente benötigt, der sollte Tails als sicherere Alternative zu einem Standard-Betriebssystem

5 siehe Kapitel *Tails Starten*

6 Es sei denn, ihr wählt explizit den unsicheren Internet Browser - ohne *Tor*. Davon raten wir dringend ab!

7 https://tor.eff.org/download/download-easy.html.en#warning

8 Ein Datenträger kann in mehrere getrennte Partitionen aufgeteilt sein.

9 Der Datenträger wird dazu ohne Schreibschutz genutzt!

in Erwägung ziehen. Diese Methode beschreiben wir im Kapitel *Persistenz*.

Systemvoraussetzungen und Betriebsarten von Tails

Tails läuft auf den meisten Rechnern, die einen „64-Bit“ Prozessor besitzen[10]. Ihr benötigt einen Rechner mit einem internen oder externen Laufwerk, das DVDs lesen und *booten* (=starten) kann, oder aber einen Rechner, der von einem USB-Stick *booten* kann.

Zusätzlich sollte euer Rechner für einen fehlerfreien Betrieb über einen Arbeitsspeicher (RAM) von mindestens 2 GB verfügen[11]. Tails läuft auf allen halbwegs aktuellen PCs und Laptops, nicht jedoch auf Smartphones (ARM-Prozessoren) oder PowerPCs (ältere Apple-Rechner).

Zumindest in zwei Fällen empfehlen wir Tails mit der Startoption **toram** zu benutzen. Dann wird das gesamte Betriebssystem von Tails mit allen Anwendungsprogrammen zu Beginn in den Arbeitsspeicher geladen. Dazu sollte euer Rechner über mindestens 2 GB Arbeitsspeicher verfügen.

1) Wenn ihr einen Tails-USB-Stick ohne mechanischen Schreibschutzschalter benutzt. Mit der Startoption **toram** können diese Datenträger nach dem Start[12] von Tails entfernt werden noch bevor ihr mit der Arbeit beginnt. Damit sind diese Datenträger vor einem eventuellen Angriff (eingeschleust über das Internet oder andere Datenträger) sicher.

2) Wenn ihr eine Tails-DVD benutzt und in eurer Sitzung Daten auf CD oder DVD brennen wollt. Mit der Startoption **toram** kann die Tails-DVD nach dem Hochfahren des Rechners herausgenommen werden. Damit ist das Laufwerk während der Sitzung frei.

Nur über Tor ins Netz

Wir gehen in diesem Kapitel darauf ein, wie Rechner im Netz kommunizieren, auf das *Tor*-Prinzip und dessen Nutzung sowie einige Fallstricke[13].

Identifizierung im Netz per IP- und MAC-Adresse

Ein großer Teil der digitale Kommunikation identifiziert die Kommunizierenden über die sogenannte IP (Internet Protocol)-Adresse. Ein *Router*, über den ihr ins Netz geht, bekommt diese **IP-Adresse** (z.B. 172.16.254.1) vom Internetanbieter zugewiesen. Die IP-Adresse wird bei jeder Netzaktivität über ein standardisiertes Protokoll (lesbar) mitgeschickt. Euer surfen, chatten oder mailen ist (ohne Tor) mit der *Identität und Lokalität dieses Routers* nachvollziehbar verknüpft.

> ***Wenn ihr keine zusätzlichen Vorkehrungen trefft, verrät die übertragene IP-Adresse den ungefähren geografischen Ort des Routers, über den ihr ins Netz geht.***

Zusätzlich besitzen alle Netzwerkadapter eine zusätzliche Kennung- die **MAC-Adresse** (z.B. B4:89:91:C1:F4:CE). Jede Netzwerkschnittstelle (z.B. die WLAN-Karte oder das kabelgebundene LAN) eures Rechners meldet sich mit einer eigenen, eindeutigen (physikalischen) MAC-Adresse (Media-Access-Control) beim Router an. Beim aktuell (noch) verwendeten Internetprotokoll (ipv4) wird diese jedoch nicht *„nach draußen“* (ins Netz) übertragen[14].

Aber: Wenn ihr z.B. per WLAN in einem öffentlichen Café ins Netz geht, kann der Betreiber oder ein Angreifer ohne technischen Aufwand eure MAC-Adresse mitprotokollieren. Damit ist dann eure Internet-Aktivität nicht mehr nur dem WLAN-Router des Cafés, sondern exakt dem von euch verwendeten WLAN-Adapter eures Computers zuzuordnen! Auch zu Hause kann ein Angreifer, der sich in euren Router hackt, unterscheiden, welcher Rechner (z.B. in der WG) eine bestimmte Mail verschickt hat. Wir kommen gleich dazu, wie ihr euch gegen eine Identifikation per MAC-Adresse schützen könnt.

Das *Tor*-Prinzip (The Onion Router)

Statt in eurem Standard-Browser z.B. die Webseite *http://tagesschau.de* direkt zu besuchen und dieser beim Kontaktaufbau die IP-Adresse eures Routers mitzuteilen, geht ihr beim voreingestellten *Tor-Browser* von Tails einen Umweg über drei Zwischenstationen. Diese drei Rechner werden von der *Tor*-Software aus weltweit (derzeit) über 7000 verfügbaren *Tor*-Rechnern *zufällig* ausgewählt.

Der Inhaber des Servers, auf dem die Zielwebseite liegt (oder ein dort mitlesender Schnüffler) erhält nicht eure IP-Adresse, sondern die vom *Tor*-Exit-Rechner **3** als Besucher*innen-IP. Zwar ist erkennbar, dass es sich hierbei um einen Rechner des *Tor*-Netzwerkes handelt (die Liste aller verfügbaren *Tor*-Rechner ist öffentlich einsehbar), aber eure Identität ist nicht rekonstruierbar, es sei

---

10 Intel oder AMD. Diese Einschränkung besteht seit Tails Version 3.0..

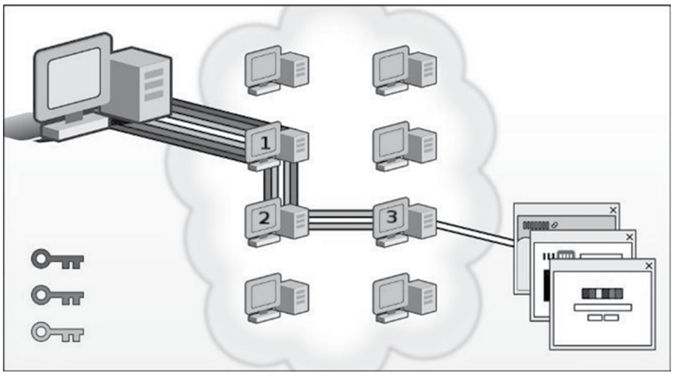
11 Bei weniger als 2 GB Arbeitsspeicher kann der Rechner manchmal „einfrieren“. Der Grund dafür liegt darin, dass Tails selbstverständlich nicht auf die sogenannte Auslagerung-Partition (SWAP) der Festplatte zurückgreifen darf: Ein Auslagern von Daten und Programmen auf die Festplatte würde ja nachvollziehbare Datenspuren hinterlassen!

12 Sobald sich der Rechner (nach Boot- und Start-Bildschirm) mit der Tails-Arbeits-Oberfläche meldet.

13 https://tor.eff.org/download/download-easy.html.en#warning

14 Bei dem neueren Internetprotokollstandard *ipv6* kann die MAC-Adresse in der IP mitkodiert werden. Das würde die Verschleierung des verwendeten Rechners gefährden. Deshalb verwendet Tails diesen Protokollstandard nicht!

denn, der Inhalt eurer Kommunikation mit der Zielwebseite verrät euch (persönliche Identifikation). Keiner der drei TOR-Rechner kennt den kompletten Pfad von eurem Rechner bis zum Zielserver. Nur ein Angreifer, der den Netzverkehr von TOR-Rechner **1** *und* **3** (aus derzeit über 7000 möglichen) mitprotokolliert, kann eure IP mit dem Besuch der Ziel-Webseite in Verbindung bringen[15].



Verschleierung der Identität bedeutet nicht automatisch Verschlüsselung

Die Verbindungen von eurem Rechner zum TOR-Rechner **1**, sowie **1—2** und **2—3** sind verschlüsselt. Damit ist der Inhalt bei einem Schnüffel-Angriff auf diese Verbindungen, bzw auf die TOR-Rechner **1** und **2** nicht lesbar. *Die Verbindung von* **3—Ziel** *ist hingegen unverschlüsselt!*

Nur wenn Ihr eine Webseite beginnend mit HTTP**S** besucht wie z.B. http**s**://linksunten.indymedia.org ist auch der Inhalt dieser letzten Verbindung verschlüsselt. Der TOR-Browser von Tails versucht immer eine HTTP**S**-Verbindung zum Ziel aufzubauen. Bietet der Webseitenbetreiber jedoch nur HTTP-Verbindungen an, ist eure Kommunikation mit diesem Server unverschlüsselt und kann dort bzw. auf dem TOR-Exit-Rechner **3** oder dazwischen mitgelesen werden!

Verschiedene Nutzungsmodelle von *TOR*

TOR verschleiert eure IP-Adresse mit der ihr zum Surfen, Mailen oder Chatten mit anderen Servern Kontakt aufnehmt. Einer der Zwecke von TOR liegt in der **Verschleierung der eigenen Identität**.

Als Besucher*in einer Webseite geht das, solange ihr dort keine Daten über euch preisgebt, oder spezifische Inhalte euch eindeutig identifizieren. Beim Mailen können euch Mail-Kontakte oder Mail-Betreffzeile leicht verraten, selbst wenn ihr peinlich genau darauf geachtet habt, dass (inklusive Account-Eröffnung) über die gesamte Historie der Account-Nutzung alles anonym ablief.

Deshalb wird vielfach behauptet, dass TOR unsinnig ist wenn ihr euch persönlich (ohne Pseudonym bei eurer Bank einloggt oder eine Mail von einer Adresse verschickt, die mit eurer Person eindeutig in Verbindung steht. Das stimmt nur zur Hälfte. Richtig ist, dass ihr mit einem (realen) persönlichen *login* eure Identität gegenüber dem Server offenbart – da hilft auch kein TOR. Aber ihr könnt auch in diesen Fällen TOR zur **Verschleierung eures Aufenthaltsortes** nutzen. Ein weiterer Anwendungsfall für TOR ist das **Erschweren von Zensur und Überwachung eurer Netzwerkaktivitäten**.

> ***Wir raten euch, IMMER per TOR ins Netz zu gehen und eure Netzaktivitäten entlang verschiedener Identitäten „aufzutrennen“.***

Identitäten sauber trennen

Es ist nicht ratsam, in ein und derselben Tails-Sitzung verschiedene Aufgaben im Internet zu erledigen, die nicht miteinander in Verbindung gebracht werden sollen. Ihr müsst selbst verschiedene (kontextuelle) Identitäten sorgsam voneinander trennen!

Ein Beispiel: Es ist gefährlich, in der gleichen Sitzung per TOR (ortsverschleiernd) die persönlichen Mails abzurufen und anonym bei indymedia einen Text zu publizieren. Das heißt, ihr solltet nicht gleichzeitig *identifizierbar* und *anonym* ins TOR-Netz. Ihr solltet auch nicht gleichzeitig unter Pseudonym A und Pseudonym B ins TOR-Netz gehen, denn diese Pseudonyme könnten auf einem überwachten/korrumpierten TOR-Exit-Rechner **3** miteinander in Verbindung gebracht werden.

Da ihr euch nicht in allen Fällen auf die Funktion *„Neue Identität“* im TOR-Browser verlassen könnt, um die verschiedenen Netzaktivitäten (durch verschiedene IP-Adressen der verschiedenen TOR-Exit-Rechner) voneinander zu separieren, lautet die unbequeme aber sichere Empfehlung:

> ***Tails zwischen Netzaktivitäten unterschiedlicher Identität herunterfahren und neu starten!***

Denn sogenannte *Cookies*[16], ein TOR-Anwendungsfehler eurerseits oder eine (noch nicht bekannte oder behobene) Sicherheitslücke in einem Programm innerhalb von Tails könnten Informationen über Eure Tails-Sitzung offenlegen. Diese könnten offenbaren, dass ein und dieselbe Person hinter den verschiedenen Netzaktivitäten der gleichen Tails-Sitzung (trotz wechselnder IP-Adresse des TOR-Exit-Rechners **3**) steckt.

15 Ein Angriff über eine sogenannte Timestamp-Analyse kommt ohne Kenntnis des Datenverkehrs von TOR-Rechner **2** aus.

16 Cookies sind kleine Dateien, die z.B. ein Webseitenbetreiber auf eurem Rechner als Webseitenbesucher zur Wiedererkennung von bestimmten Einstellungen ablegt. Tails untersagt das Speichern der meisten Cookie-Sorten. Andere, zugelassene Cookies verbleiben im flüchtigen Arbeitsspeicher und verschwinden bei einem Neustart.

Website Fingerprinting erschweren

Wenn ihr eine Webseite über euren Browser anfordert, wird diese in kleinen Paketen, die sich durch eine bestimmte Größe und zeitliche Abfolge auszeichnen (und weiteren Charakteristiken), an euch übertragen. Auch bei der Nutzung von *Tor* kann die Abfolge der übertragenen Pakete analysiert und bestimmten Mustern zugeordnet werden. Die Muster können hier mit denen von überwachten Seiten aus dem Netz abgeglichen werden. Um diese Analyse-Methode zu erschweren und eure Spuren zu verschleiern, hilft folgendes: Öffnet vor dem Aufruf der gewünschten Webseite diverse andere Seiten in weiteren *Tabs* eures Browserfenster. Dadurch entsteht eine Menge von weiterem Traffic der die Analyse eures Musters erschwert[17].

Ist *Tor* noch sicher?

Diese Frage scheint einfach, ist aber schwierig zu beantworten, weil sie eine Angreifer*in mit einbezieht - wem gegenüber ist *Tor* sicher? Eure Arbeitgeber*in wird *Tor* vermutlich nicht knacken können, das gleiche gilt wahrscheinlich auch für lokale und nationale Polizeibehörden. Bei Geheimdiensten sind wir mit Aussagen über die Sicherheit vorsichtiger.

Es ist bekannt, dass Geheimdienste *Tor* attackieren, um die Anonymität der Nutzer*innen aufzuheben. Wir analysieren im Kapitel „Warnung: Grenzen von Tails“ verschiedene Angriffe auf *Tor*. Die bislang veröffentlichten „Ermittlungserfolge“ bei der Deanonymisierung beruhten auf Sicherheitslücken der verwendeten Browser oder auf Anwendungsfehlern, die es ermöglichten, unterschiedliche Identitäten zu verknüpfen. Es sind auch Sicherheitslücken im *Tor*-Protokoll gefunden und behoben worden - allerdings ist nicht bekannt, ob diese Lücken zur Enttarnung einer User*in beigetragen haben. Es sei nochmal betont, dass *Tor* nur einen Teil des Datentransportes übernimmt und das im konkreten Anwendungsfall immer noch weitere Software nötig ist - zum Beispiel der Webbrowser oder aber auch das Betriebssystem - und dass es für eine Angreifer*in einfacher sein kann, diese Software anzugreifen, als *Tor* zu knacken.

> ***Geheimdienste attackieren das Tor-Netzwerk, um die Anonymität der Tor-Nutzer*innen zu brechen. Wir können die Effektivität von Tor nicht garantieren !***

Wir wissen, dass es massive Anstrengungen von sehr starken Angreifer*innen (NSA, FBI) gibt, sogenannte „*Tor*-hidden-services“ zu „deanonymisieren“; *Tor* kann nämlich nicht nur User*innen anonymisieren, sondern auch Server. Das ist zwar nicht die im Heft dargestellte Standard-Nutzung von *Tor*, sollte aber trotzdem ernst genommen werden, weil sich Forschungserfolge auf dem einen Gebiet vermutlich auf das andere übertragen lassen.

Absolute Sicherheit gibt es nicht und *Tor* ist zur Zeit das Beste, was es gibt, um die eigene Identität zu schützen. *Tor* wird ständig weiterentwickelt, um bekannt gewordene Schwächen zu beseitigen. Daher benutzt auf jeden Fall immer die neueste Tails-Version!

Das Ergebnis bleibt leider unbefriedigend: Erst bei Kenntnis des Versagens des *Tor*-Netzwerks sind wir in der Lage, eine klare (negative) Aussage zu treffen - das heißt, erst wenn das Kind in den Brunnen gefallen ist, können wir mit Sicherheit sagen, dass es so ist. Das bedeutet, ihr müsst bei der Bewertung etwaiger Konsequenzen von der *Möglichkeit* ausgehen, dass eure **IP-Adresse** einer Recherche oder einer Veröffentlichung zugeordnet werden *könnte*. Der Ort des Routers wäre in einem solchen Fall enttarnt. Die durch Tails veränderte **MAC-Adresse** hilft euch zumindest zu verschleiern, welcher Rechner an dem dann enttarnten Router für diese Netzaktivität verantwortlich sein soll *(siehe nächstes Kapitel).*

Da niemand kategorisch ausschließen kann, dass auch diese zusätzliche Ebene der Verschleierung technisch durchbrochen werden *könnte*, solltet ihr *zusätzlich* auf für euch kontrollierbare Sicherungsmethoden zurückgreifen. Zu zwei dieser Methoden raten wir bei besonders sensiblen Aktivitäten im Internet: Geht nicht von einem für euch gewöhnlichen Ort ins Netz und nutzt keinen Rechner, der euch zugeordnet werden kann (d.h. nicht übers Internet, sondern so anonym wie möglich *offline* besorgt).

Damit ergeben sich dann folgende Sicherungsebenen zur Anonymisierung *besonders sensibler Netzaktivitäten*:

> **1) Sichere Konfiguration der jeweiligen Anwendungsprogramme** *(in dieser Anleitung)*
>
> **2) Verschleierung der IP-Adresse per Tor**
>
> **3) Verschleierung der MAC-Adresse per Tails** *(siehe nächstes Kapitel)*
>
> **4) Netzzutritt an einem für euch ungewöhnlichen Ort ohne Kameras, ohne euer Handy/ andere WLAN-, oder Bluetooth-Geräte**
>
> **5) Anonymer Kauf und versteckte Lagerung eines „Recherche-Computers“**

17 http://arxiv.org/pdf/1512.00524v1.pdf

Tails ändert eure MAC-Adresse(n)

WLAN ständig auf der Suche nach verfügbaren Netzen

Wenn ihr mit angeschaltetem Laptop, Tablet oder Smartphone bei aktiviertem WLAN[18] durch die Stadt geht, dann meldet sich eure WLAN-Karte mit ihrer MAC-Adresse bei allen WLAN-Routern in Funkreichweite. Und das, ohne dass ihr im Netzwerk-Manager eine solche Verbindung aktiv auswählt und herstellt! Die Router aller dort gelisteten WLAN-Netze der Umgebung haben euren Computer bereits über dessen WLAN-MAC-Adresse bei einer *initialen* Begrüßung identifiziert! Ihr hinterlasst also eine zurückverfolgbare Spur, falls diese flüchtigen „Begrüßungen" aufgezeichnet werden[19].

Im Falle eines Anwendungsfehlers oder sonstigen Tor-Problems könnte ein Angreifer euren Rechner anhand der aufgezeichneten MAC-Adresse des WLANs identifizieren, sofern er sich Zugang zum Router verschafft, über den ihr ins Netz gegangen seid.

> ***Zur zusätzlichen Sicherheit ersetzt Tails vor der ersten Netzeinwahl (beim Start von Tails) die MAC-Adresse(n) aller im BIOS aktivierten Netzwerkadapter eures Rechners durch zufällige Adressen.***

Es gibt allerdings Situationen, in denen das nicht funktioniert: Manche Netzwerke erlauben nur einer beschränkten Liste von voreingestellten MAC-Adressen den Zugang. Nur, wenn ihr glaubt, auf diese zusätzliche Sicherheit verzichten zu können, könnt ihr Tails neu starten und beim Tails-Begrüßungsfenster *„Ja"* (für weiter Optionen) anklicken und dann die (standardmäßig gesetzte) Option *„Alle MAC-Adressen manipulieren"* abwählen! **Wir raten jedoch zugunsten eurer Anonymität davon ab!**

Vorsicht beim UMTS-Stick

Auch das ist ein eigenständiger Netzwerkadapter, der somit auch eine eigene MAC-Adresse besitzt. Auch diese wird von Tails beim Start mit einer Zufallsadresse überschrieben. Dennoch muss man hier auf die zusätzliche Sicherheit einer veränderten MAC-Adresse verzichten, da auch die eindeutige Identifikationsnummer eurer SIM-Karte (**IMSI**) und die eindeutige Seriennummer eures Sticks (**IMEI**) *bei jeder Netzeinwahl an den Mobilfunkanbieter übertragen* werden und eine Identifikation sowie eine geografische Lokalisierung ermöglichen. Der UMTS-Stick funktioniert wie ein Mobiltelefon!

Wer nicht möchte, dass verschiedene Recherche-Sitzungen miteinander in Verbindung gebracht werden können, darf weder den UMTS-Stick noch die SIM-Karte mehrmals benutzen![20]

> ***Für sensible Recherchen oder Veröffentlichungen sind sowohl der UMTS-Stick als auch die SIM-Karte zu entsorgen.***

Andernfalls wären verschiedene Recherchen über die gemeinsame IMEI oder die gemeinsame IMSI miteinander verknüpft. *Der Austausch der SIM-Karte allein genügt ausdrücklich nicht!*

Wir legen euch einige weitere Anmerkungen zu den Grenzen von Tails (im Anhang) ans Herz! Nach diesen Vorüberlegungen und Warnungen zur Sicherheit im Netz wird es nun praktisch.

Tails starten

Wir gehen in diesem Kapitel davon aus, dass ihr einen aktuellen *Tails-USB-Stick* oder eine *Tails-DVD* habt. **Wie ihr das Tails-Live-System herunterladen und überprüfen! könnt**, um ein solches Start-Medium zu erzeugen, **beschreiben wir im Anhang** dieser Anleitung. Wir gehen ebenfalls davon aus, dass euer Computer bereits so eingestellt ist, dass er von einem der drei Medien *booten* (=starten) kann. Auch diese minimale **Einstellung im BIOS** ist **im Anhang** beschrieben.

Tails booten

Wenn ihr auf die Sicherheit durch die im vorigen Kapitel beschriebene Veränderung der MAC-Adresse eures WLANs setzen wollt, **dann muss der Tails-Datenträger vor dem Start eingelegt/eingesteckt sein – andernfalls würde ein „Fehlstart" mit eurem Standard-Betriebssystem euren Laptop per originaler MAC-Adresse eures WLANs in der Funkreichweite bekannt machen!**

Bei den meisten Computern genügt es, beim wenige Sekunden später erscheinenden **Boot-Bildschirm** die voreingestellte Auswahl *Live* mit der Enter-Taste zu bestätigen oder zehn Sekunden zu warten. Nur wenn Tails danach keine sichtbaren Startbemühungen unternimmt, solltet ihr in einem neuen Start-Versuch die Option *Tails (Troubleshooting Mode)* auswählen.

18 Das WLAN lässt sich bei TAILS wie bei allen Betriebssystemen über den Netzwerk-Manager an- und abschalten, sofern ihr es nicht im BIOS deaktiviert habt.

19 In der Standard-Einstellung der Router werden solche Ereignisse nicht mitprotokolliert. Werbeanbieter*innen nutzen allerdings genau diese Möglichkeit, um potentielle Kund*innen vor dem Schaufenster oder im Laden zu identifizieren und ihre Verweildauer zu messen – mit ganz normaler Hardware!

20 Das gilt auch bei anonymem Erwerb von UMTS-Stick und SIM-Karte und deren anonymer Freischaltung.

Mac-Nutzer*innen müssen beim booten die Alt-Taste gedrückt halten und anschließend Tails als Startvolume auswählen.

> *Ein spezieller Recherche-Computer, aus dem ihr die Festplatte ausbaut und den ihr damit nur für Live-Systeme wie Tails nutzbar macht, löst das „Fehlstart“-Problem und verhindert zudem ein „versehentliches“ Speichern von Daten auf die Festplatte!*

Zusätzliche Boot-Optionen

Um (eine) zusätzliche Boot-Option(en) auszuwählen, müsst ihr hingegen bei Erscheinen des Boot-Bildschirms

1. die *Tabulator*-Taste  drücken und
2. ein *Leerzeichen* eingeben. Dann die jeweilige(n) Boot-Option(en jeweils durch ein Leerzeichen getrennt) eingeben und mit *Enter* abschließen:



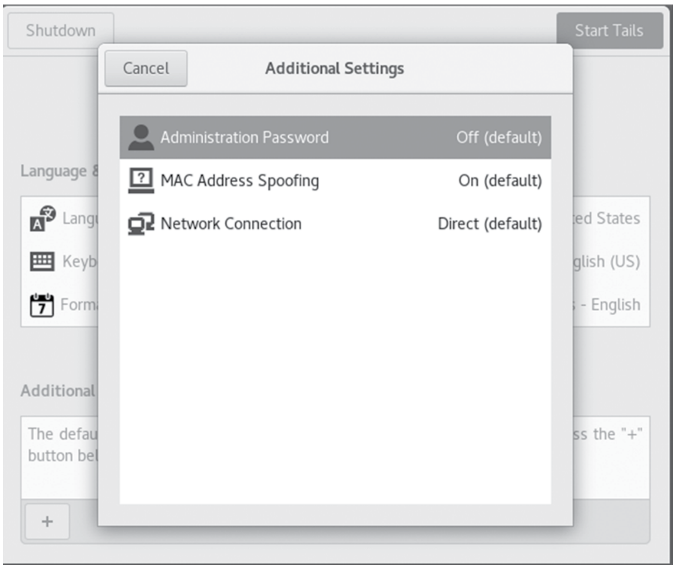
- **toram** - lädt Tails komplett in den Arbeitsspeicher (mindestens 2 GB). Empfehlenswert, wenn ihr *a)* einen USB-Stick ohne Schreibschutzschalter als Tails-Boot-Medium verwendet oder *b)* eine Tails-DVD nutzt, das DVD-Laufwerk aber zum Brennen von Daten in der Sitzung benötigt.

Tails-Startbildschirm



Nach erfolgreichem Boot-Vorgang erscheint folgender Startbildschirm, bei dem ihr durch Auswahl der Option *„Deutsch“* (links unten) auf eine deutsche Tastaturbelegung und deutschsprachige Menüs umschalten könnt.

Durch die Auswahl *Ja* und *Vorwärts* bei *„weitere Optionen?“* habt ihr folgende weitere Start-Optionen:



- **Festlegen eines Administrations-Passworts** - das benötigt ihr, wenn ihr für ein Programm Administrator-Rechte braucht. Dies ist z.B. notwendig für das Installieren eines Druckers oder den Zugriff auf die interne Festplatte des Rechners. Ihr könnt euch im dann folgenden Dialog ein beliebiges Passwort ausdenken (und merken!). Es behält seine Gültigkeit nur für diese eine Tails-Sitzung.
- **Manipulation aller MAC-Adressen ausschalten** Wenn der Netzzugang nur bestimmten Computern gewährt wird und ihr auf die zusätzliche Sicherheit einer geänderten MAC-Adresse verzichten könnt[21],

21 Bitte lest dazu die Hinweise im Kapitel T*ails ändert eure MAC-Adresse.*

könnt ihr das standardmäßig gesetzte Häkchen wegnehmen.

- **Alle Netzwerkfuktionen deaktivieren**
  Hiermit bleiben alle Netzwerkadapter softwareseitig beim Start deaktiviert. Dies geschieht sinnvoller Weise, *bevor* Tails seine Netzwerkfunktionalität startet. So bleiben u.a. WLan und Bluetooth still und können eure Anwesenheit in Funkreichweite anderer Geräte nicht mehr preisgeben. (siehe dazu das Kapitel *Tails als Quasi-Schreibmaschine*).

Nachdem ihr den Schalter *Start Tails* angeklickt habt, meldet sich Tails mit der grafischen Oberfläche und den zwei Hauptmenüs **Anwendungen, Orte.** Damit Tails erkennt, ob ihr eine veraltete Version benutzt, wird zu Beginn euerer Sitzung (nach erfolgreich hergestellter Netzwerk-Verbindung) einmal nach Hause telefoniert. Ihr werdet ggfs. aufgefordert, per *Upgrade* eine neue Version einzuspielen. Wie das geht, erläutern wir im Anhang im Kapitel *Tails-Installer* bzw. *Tails-Upgrader.*

Zur gleichzeitigen Arbeit mit mehreren Programmen sind zwei Arbeitsflächen voreingestellt - damit es auf einem kleinen Bildschirm nicht zu voll wird. Zieht den Mauszeiger in die linke obere Ecke, um eine Übersicht über den aktuellen Desktop, Arbeitsflächen und das Programmpanel zu bekommen.

Tails benutzt die graphische Oberfläche *Gnome*, deren Benutzung etwas Einarbeitung bedarf. Insbesondere ist die Standardeinstellung für das Scrollen MacOSX nachempfunden und damit genau andersrum als von Windows und den meisten Linuxen gewohnt.

Datenträger werden nicht automatisch „geöffnet"

Anders als ihr es gewohnt seid, wird ein eingelegter/eingesteckter externer Datenträger nicht automatisch geöffnet und damit verfügbar gemacht. Ihr sollt damit (absichtlich) die Kontrolle über alle Datenorte behalten und nicht aus Versehen doch etwas auf die Festplatte speichern!

> ***Datenträger werden erst über das aktive Anwählen (linker Mausklick) unter „Orte ▸ Rechner" in das System eingebunden. Vorher können von/auf ihm keine Daten gelesen/gespeichert werden.***
>
> ***Bevor ihr den Datenträger nach fertiger Arbeit abziehen könnt, müsst ihr ihn unter „Orte ▸ Rechner" mit der rechten Maustaste anklicken und dann „Laufwerk sicher entfernen" wählen!***

Tails Programme

Das Tails-Live-System ist eine Zusammenstellung von vielen Programmen auf der Basis eines *Debian-Linux*. Alle Programme zu erläutern, erfordert viel zu viel Platz – selbst wenn wir nur deren grundlegende Handhabung beschreiben würden. Daher hier nur die Links zu Anleitungen für die wichtigsten Tails-Programme:

Surfen	Tor-Browser	https://tails.boum.org/doc/anonymous_internet/Tor_Browser/index.en.html
Mailen	Thunderbird	https://de.wikipedia.org/wiki/Mozilla_Thunderbird
Chatten	Pidgin + OTR	https://tails.boum.org/doc/anonymous_internet/pidgin/index.en.html
Office	LibreOffice	http://wiki.ubuntuusers.de/LibreOffice
Gemeinsames Schreiben	Gobby	https://gobby.github.io/
Layout+Satz	Scribus	http://www.scribus.net/
Videos abspielen	Video	http://wiki.ubuntuusers.de/Totem
Grafikbearbeitung	Gimp	http://wiki.ubuntuusers.de/GIMP
Tonbearbeitung	Audacity	http://wiki.ubuntuusers.de/Audacity
Videobearbeitung	Pitivi	http://wiki.ubuntuusers.de/PiTiVi
Newsfeeds lesen	Liferea	http://wiki.ubuntuusers.de/Liferea
Bitcoins	Electrum	https://tails.boum.org/doc/anonymous_internet/electrum/index.en.html
Anonymer Datenaustausch	Onion–Share	https://onionshare.org/
Metadaten entfernen	MAT	https://mat.boum.org/
Scannen	Simple scan	http://wiki.ubuntuusers.de/Simple_Scan
CD/DVD brennen	Brasero	http://wiki.ubuntuusers.de/Brasero
Passwortverwaltung	KeepassX	http://wiki.ubuntuusers.de/KeePassX

Netzwerkverbindung herstellen

Tails sucht nach dem Start selbständig nach verfügbaren Netzwerkverbindungen. Wenn ihr beim Start von Tails ein Netzwerkkabel eingesteckt habt und euer LAN-Zugang nicht Passwort-geschützt ist, dann startet Tor automatisch. Der Aufbau eines Tor-Netzwerks mit der dazu notwendigen Synchronisation der Systemzeit dauert eine Weile – bei Erfolg erscheint die Meldung, *„Tor ist bereit. Sie haben jetzt Zugriff auf das Internet"* Ab jetzt werden alle Surf-, Chat-, Mail-Verbindungen durch das Tor-Netz geleitet.

Für eine (in der Regel Passwort-gesicherte) WLAN-Verbindung könnt ihr den Netzwerkmanager in der oberen Kontrollleiste anklicken oder über das Menü *Anwendungen* ▸ *Systemwerkzeuge* ▸ *Einstellungen* ▸ *Netzwerk* und Verschlüsselungsart auswählen und dann das Passwort eingeben.

Surfen über Tor

Wenn der Netzwerkmanager von Tails eine Netzwerkverbindung hergestellt hat, könnt ihr den TOR-Browser starten. Entweder per Klick auf das Symbol in der Kontrolleiste oben links, oder im Menü:
Anwendungen ► Internet ► TOR-Browser.

Skripte verbieten – NoScript

Es gibt aktive Inhalte auf Webseiten, die eure Anonymität gefährden können. Oft nutzen Webseiten Javascript, Java-Applets, Cookies, eingebettete Flash- oder Quicktime-Filmchen, PDF-Dokumente oder nachzuladende Schriften. Derartige *aktive* Webseiteninhalte können über einen so genannten „Fingerprint" viele Einstellungen und Charakteristika eures Rechners übertragen (Prozessor, Bildschirmauflösung, installierte Schriften, installierte Plugins, etc.), sodass ihr im ungünstigen Fall doch identifizierbar seid[22]. Die TOR-Installation von Tails kümmert sich um die Deaktivierung vieler dieser Inhalte. Wir empfehlen jedoch, gleich zu Beginn eurer Netzaktivitäten eine noch restriktivere Einstellung in eurem TOR-Browser vorzunehmen:

> ***Mit dem NoScript-Button im TOR-Browser alle Skripte verbieten!***

Im voreingestellten TOR-Browser von Tails sind *Skripte* und *Plugins* zunächst erlaubt.

Mit der Option *NoScript* (Button in der Browser-Kontrollleiste) verbietet ihr zunächst alle! Skripte global. Empfehlenswert ist, Skripte bei den besuchten Webseiten (und ihren Unterseiten) jeweils *erst dann* zuzulassen, wenn es für eure Aktivität notwendig ist- wenn also etwas auf der jeweiligen Webseite „nicht wie gewohnt funktioniert". Beachtet, dass ihr dadurch eure Anonymität verlieren könnt!

Im neuen TOR-Browser könnt ihr über einen Klick auf die kleine grüne Zwiebel in der Steuerleiste des Browsers das Sicherheitslevel anpassen. Hier stehen Euch drei Voreinstellungen zur Verfügung. Auf dem niedrigsten Level funktionieren auch Seiten mit aktiven Inhalten.

Download aus dem Netz

Es ist kein Fehler, sondern Absicht, dass ihr über den TOR-browser Dateien nur in das Verzeichnis *TOR Browser* (im Verzeichnis *Persönlicher Ordner*) speichern dürft. Das bewahrt euch vor unbeabsichtigtem Fehlspeichern. Falls ihr Daten auf den Desktop oder einen Datenträger speichern wollt, müsst ihr in einem zweiten Schritt die Daten an den Zielort kopieren. Dazu eignet sich der Dateimanager unter *Anwendungen ► Zubehör ► Dateien*.

In Ausnahmefällen ohne *TOR* ins Netz ?

Einige öffentliche WLAN-Zugänge in Cafés, Universitäten, Büchereien, Hotels, Flughäfen, etc. leiten Webseitenanfragen um auf spezielle Portale, die ein *login* erfordern. Solche Zugänge sind nicht über *TOR* erreichbar.

> ***Wir raten dringend von der Nutzung des Browsers ohne TOR ab!***

Nur wenn ihr auf die Verschleierung eurer Identität und auf die Verschleierung eures Standortes verzichten wollt und könnt, gibt es in Tails die Möglichkeit auch ohne! *TOR* ins Netz zu gehen. Bedenkt, dass euch alles, was ihr damit „ansurft", zugeordnet werden kann. Ihr könnt den unsicheren Browser starten über:
Anwendungen ► Internet ► Unsicherer Browser.

> ***Auf keinen Fall solltet ihr diesen „nackten" Browser parallel zum anonymen TOR-Browser nutzen. Das erhöht die Angreifbarkeit und die Verwechslungsgefahr mit eventuell katastrophalen Konsequenzen!***

Daten verschlüsselt aufbewahren

Wie bereits erwähnt, Tails speichert nichts auf eurer Festplatte, es sei denn, ihr verlangt dies explizit durch die Auswahl der Festplatte im Menü *Orte ► [Name der Festplatte]*. Nach dem Ausschalten des Rechners gehen alle Daten verloren. Ihr solltet daher einen **Daten-USB-Stick** zur Aufbewahrung eurer Daten nutzen. Aus Sicherheitsgründen sollte dieser *nicht identisch mit dem* (möglichst schreibgeschützten) *Tails-Betriebssystem-Stick* sein!

Da wir grundsätzlich alle Daten verschlüsselt aufbewahren, legen wir auf einem neuen Daten-USB-Stick eine *verschlüsselte Partition* an. Tails nutzt die Linux-Verschlüsselungssoftware *dm-crypt*. Ihr könnt die Daten dann auf allen Linux-Betriebssystemen entschlüsseln. **Ein Datenaustausch mit Windows- oder MAC OS X Betriebssystemen ist damit allerdings nicht möglich!**

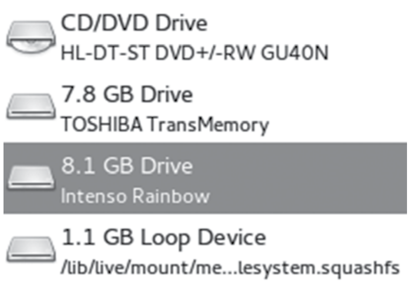
Verschlüsselte Partition auf einem Datenträger anlegen[23]

1. **Laufwerksverwaltung starten**
   Anwendungen ► Hilfsprogramme ► Laufwerke
   Die Laufwerksverwaltung listet alle derzeit verfügbaren Laufwerke und Datenträger.

22 https://panopticlick.eff.org/

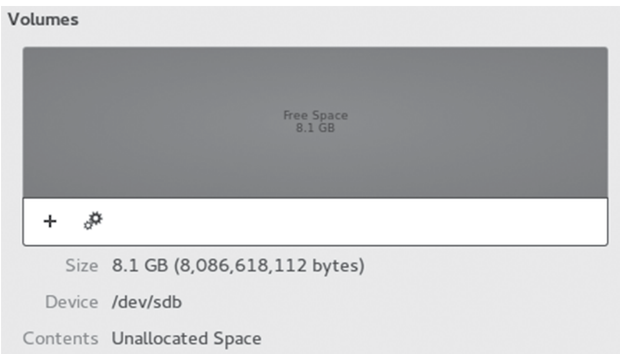
23 Weiterführende Infos: https://tails.boum.org/doc/encryption_and_privacy/encrypted_volumes/index.en.html

2. **Daten-USB-Stick identifizieren**
Wenn ihr den neu zu verschlüsselnden USB-Stick jetzt einsteckt, sollte ein neues „Gerät“ in der Liste auftauchen. Wenn ihr draufklickt, seht ihr die Details des Datenträgers. Überprüft genau, ob ihr den richtigen Datenträger ausgewählt habt (blau hinterlegt) - ob also die Beschreibung (Marke, Name, Größe) mit eurem Gerät übereinstimmt! Eine Verwechslung mit einem anderen Datenträger wird diesen löschen.



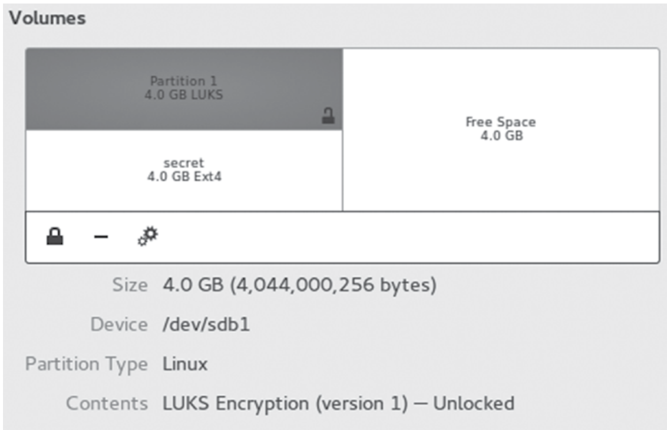
3. **Platz schaffen**
Nach dem Auswählen des USB-Sticks erscheint auf der rechten Seite ein Darstellung der Partitionen. Wenn dort kein „Freier Platz“ mehr angezeigt wird, müsst ihr bestehende Partitionen löschen. Dazu wählt ihr die betroffene Partition aus, klickt auf den „Minus“-Button und bestätigt das Löschen. Wir empfehlen, alle Partitionen zu löschen und keinen Mischbetrieb von verschlüsselten und unverschlüsselten Daten auf dem gleichen Stick zu versuchen, um Verwechselungen zu vermeiden

4. **Eine verschlüsselte Partition erzeugen**
Jetzt zeigt das Fenster einen leeren Datenträger.



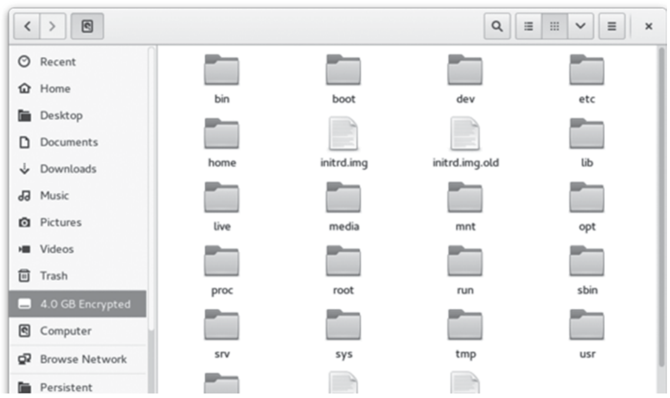
Klickt nun auf den Button + Partition erstellen. Es erscheint ein Menü „Partition erstellen“, in dem ihr die neue Partition festlegen könnt.

- **Größe:** Ihr könnt die Größe der zu verschlüsselnden Partition auch verkleinern, damit noch andere Partitionen auf dem USB-Stick Platz finden. Wir raten euch jedoch, sensible Datenprojekte *nicht mit anderen Daten auf dem gleichen Stick* zu speichern.
- **Typ:** Hier wählt ihr *„Verschlüsselt, kompatibel mit Linux-Systemen (LUKS+Ext4)“*.
- **Name**: Hier könnt ihr einen Namen für den Datenträger wählen, um ihn später identifizieren zu können. Beachtet: Dieser Name ist für alle lesbar!
- **Kennwort:** Wählt ein starkes Passwort. Das Passwort[24] sollte komplex genug sein, damit es nicht geknackt werden kann. Aber ihr müsst es euch auch merken können! Dann auf *Erstellen* klicken. Dieser Prozess kann eine Weile dauern. Wenn die Fortschrittsanzeige erlischt, seid ihr fertig.



Verschlüsselte Partition öffnen

Wenn ihr einen verschlüsselten USB-Stick einsteckt, wird er (wie alle Datenträger) in Tails *nicht automatisch* geöffnet, sondern erst, wenn ihr ihn im Menü *Orte* anwählt.

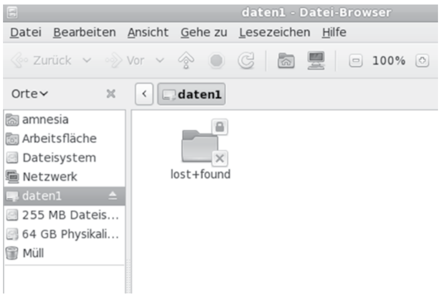


Ihr werdet aufgefordert, das Passwort einzugeben:



Wenn es das richtige Passwort ist, dann wird die Partition im Datei-Manager wie ein Datenträger mit dem von euch gewählten Namen angezeigt. Ihr könnt nun Dateien hinein kopieren oder sonstige Dateioperationen durchführen.

24 Hinweise zu einem sicheren Passwort im Anhang.



Bevor ihr den Datenträger nach fertiger Arbeit abziehen könnt, müsst ihr ihn unter *Orte ► Rechner* mit der *rechten Maustaste* anklicken und dann *Auswerfen* wählen!

Bedenken gegen TrueCrypt

TrueCrypt ist eine Software, die verschlüsselte Partitionen ermöglicht und auf Windows, MacOSX und Linux läuft, was den Datenaustausch sehr vereinfacht. Die Arbeit an *TrueCrypt* ist aber eingestellt worden. Die im Mai 2014 erschienene letzte *TrueCrypt*-Version wird von den Entwickler*innen selbst als *nicht sicher(!)* eingestuft und erlaubt nur noch das Entschlüsseln bereits vorhandener *TrueCrypt*-Container.

Um nicht in die missliche Lage zu kommen, irgendwann die alten Datenträger nicht mehr entschlüsseln zu können, raten wir, zu sichernde *TrueCrypt*-verschlüsselte Inhalte zu entschlüsseln und umzukopieren auf *dm-crypt*-verschlüsselte Datenträger (erster Abschnitt dieses Kapitels).

Veracrypt ist eine Weiterentwicklung von *TrueCrypt* und hat von dort ein paar Sicherheitsprobleme geerbt. Inzwischen sind aber alle bekannten Probleme behoben. *Veracrypt* ist noch nicht Bestandteil von Tails, wir erwähnen es der Vollständigkeit halber und weil es das einzige uns bekannte Tool ist, das betriebssystem-übergreifend einsetzbar ist.

TrueCrypt entschlüsseln

Solltet ihr trotz der zuvor dargelegten Bedenken TrueCrypt-Partitionen (Volumes) oder -Dateien (Container) zum betriebssystem-übergreifenden Datenaustausch verwenden, bietet dm-crypt nur noch die Möglichkeit zum **Lesen** der Partition bzw. des Datei-Containers. Dazu gibt es jedoch kein Programm mit einer grafischen Oberfläche. Ihr müsst ein sogenanntes *Root-Terminal* über *Anwendungen ► Systemwerkzeuge ► Root-Terminal* öffnen (dazu müsst ihr beim Tails-Startbildschirm ein Passwort festlegen) und dann einige Linux-Kommandos eingeben. Die Anleitung dazu findet ihr in der Tails-Dokumentation unter *Opening TrueCrypt volumes using cryptsetup*[25].

25 Aktuell zu finden unter: https://tails.boum.org/doc/encryption_and_privacy/truecrypt/index.de.html

Identifikation von externen Datenträgern

Jeder externe Datenträger *(Festplatte oder USB-Stick)* wird von der Laufwerksverwaltung des Betriebssystems (Linux, Windows und auch MAC OS X) identifiziert und registriert. Die Nutzung eines solchen Datenträgers unter Tails hinterlässt KEINE Spuren, da alle Protokoll-Dateien beim Ausschalten des Rechners aus dem (flüchtigen) Arbeitsspeicher verschwinden und dieser zusätzlich mit Zufallszahlen überschrieben wird, aber:

> ***Wenn ihr einen Datenträger (auch) an einem Rechner OHNE Tails benutzt, dann besteht die Gefahr, dass sich dieser Rechner über eine eindeutige Identifikationsnummer an diesen Datenträger „erinnert“.***

Bei einer Beschlagnahmung des Rechners bzw. einer feindlichen Übernahme lässt sich damit nachvollziehen, dass und wann z.B. ein bestimmter USB-Stick zum Einsatz kam[26]. Die eindeutig identifizierbaren Spuren in den System-Protokolldateien „verbinden“ also euren USB-Stick mit allen Rechnern in denen er jemals gesteckt hat. Wir erzählen das, weil wir damit deutlich machen möchten:

> ***Datenträger, die zum Speichern eines sensiblen Dokuments benutzt wurden, müssen (z.B. nach dessen Veröffentlichung) vollständig gelöscht und vernichtet werden.***

Wie das geht, erfahrt ihr im nächsten Kapitel.



Daten löschen

Es ist leider sehr kompliziert, einmal erzeugte Daten „sicher“ loszuwerden. Alle wissen vermutlich, dass es mit dem normalen Löschen einer Datei nicht getan ist – die Datei bleibt vollständig erhalten, ihr Name wird lediglich aus der Liste verfügbarer Dateien auf diesem Datenträger ausgetragen. Der belegte Platz wird freigegeben, aber nicht überschrieben.

Leider führen aber auch Software-Techniken, die einzelne Bereiche eines Datenträgers mit verschiedenen Datenmustern mehrfach überschreiben zumBeispiel bei USB-Sticks nicht zum gewünschten Ergebnis!

26 Umgekehrt gilt das nicht: Ein (nicht gehackter) USB-Stick merkt sich nicht, in welche Rechner er gesteckt wurde.

Für Ungeduldige auch hier gleich das Ergebnis unser Ausführungen vorweg:

> ***Die sicherste Variante ist, Daten nur (temporär) im Arbeitsspeicher zu halten!***
>
> ***Wenn Daten dauerhaft gesichert werden müssen, dann muss es a) ein externer Datenträger sein und dieser muss b) komplett verschlüsselt sein. Ein sicher verschlüsselter Datenträger ist der beste Schutz gegen (lesbare) Überreste.***
>
> ***Löschprogramme wie z.B. wipe funktionieren auf Flash-Medien (USB-Sticks, SD-Karten, SSD, etc) prinzipbedingt nicht zuverlässig. Selbst wenn das Medium als Ganzes überschrieben wird, können Reste zurückbleiben. Deshalb c) zerstören wir Medien mit hochsensiblen Inhalten zusätzlich.***

Probleme beim Überschreiben von Datenträgern

Physikalische Eigenschaften der Datenträger erlauben es, den ehemaligen Inhalt einer überschriebenen Speicherstelle zu rekonstruieren. Wir ersparen euch hier Details und erläutern lieber, warum es dabei weniger um die Anzahl der Überschreibvorgänge geht!

Bei **magnetischen Festplatten** gibt es das Problem, dass defekte Sektoren (=Speicherbereiche) von der Festplattensteuerung aussortiert werden und ehemals dort gespeicherte Daten umkopiert werden. Ein Überschreib-Programm zum „sicheren" Löschen hat dann auch keinen Zugriff mehr auf diese defekten Sektoren. Im Forensik-Labor hingegen lassen sich diese Bereiche auslesen – mit unter Umständen fatalen Folgen für euch.

Bei sogenannten Flash-Speichermedien wie z.B. **USB-Sticks, SD-Karten, CompactFlash-Karten und die neueren SSD-Festplatten (Solid-State-Disks)** ist dieses Problem des internen Umkopierens (außerhalb der Kontrolle des Anwenders) wegen der besonders hohen Fehleranfälligkeit des Speichers kein Ausnahmefall, sondern die Regel[27]. Eine Überschreibeprozedur zum „sicheren" *Löschen einzelner Dateien* „erwischt" dann nur eine von mehreren Kopien. Eine der neueren Forschungsarbeiten bescheinigt sämtlichen Software-Löschtechniken, dass sie angewendet auf Flash-Speicher selbst beim **Überschreiben des gesamten Speichermediums nur unzuverlässig** funktionieren[28].

---

27 Zur ausgewogenen Belastung der Speicherstellen werden Bereiche ständig umkopiert. Mehr als zehn versteckte Kopien einer Datei sind keine Seltenheit bei Flash-Speicher.

28 Michael Weie et. al.: „Reliably Erasing Data From Flash-Based Solid State Drives" 9th USENIX Conference on File and Storage Technologies. „For sanitizing entire disks, built-in sanitize commands are effective when implemented correctly, and software techniques work most, but not all, of the time. We found that none of the available software techniques for sanitizing individual files were effective." http://static.usenix.org/event/fast11/tech/full_papers/Wei.pdf

Das sichere Löschen von einzelnen Dateien hingegen gelang mit keinem der getesteten Programme!

Mit diesen Einschränkungen (als dringliche Warnung) zeigen wir euch, wie ihr bei Tails die Löschroutine *wipe* **zum Überschreiben des gesamten Datenträgers** nutzen könnt:

1. ***Datenträger im Dateimanager auswählen:*** *Orte ▸ (Name des Datenträgers)*
2. ***Im Dateimanager bei*** *Ansicht ▸ Verborgene Dateien anzeigen* ***ein Häkchen setzen***
3. ***Alle Ordner und Dateien markieren***
4. *(rechter Mausklick) ▸ Sicher löschen*
   (Die Dateien sind *für euch* ***unwiderruflich weg!)***
5. ***Im (danach leeren) Feld dieses Datenträgers:*** *(rechter Mausklick) ▸ Sicheres Löschen des verfügbaren Fesplattenspeichers*
6. ***Drei Durchläufe bei*** **zweifachem Überschreiben** ***(also sechsfach) genügen bei neueren Datenträgern - bei Unsicherheit und bei alten Festplatten könnt ihr*** *38-faches Überschreiben* ***wählen.***
7. ***Warten – je nach Größe des Datenträgers einige Minuten bis viele Stunden.***

Datenträger vernichten

Gerade wegen der Unzulänglichkeit vieler Software-Löschtechniken und der weitgehenden Möglichkeiten von forensischer Daten-Wiederherstellung solltet ihr sensible Datenträger lieber zusätzlich zerstören. Auch das ist leider problematischer als gedacht - optische Medien sind am einfachsten zu zerstören.

Magnetische Festplatten sind sehr schwer zu zerstören. Ihr könnt sie nicht einfach ins Feuer werfen. Die Temperaturen, die ihr damit an den Daten-tragenden Scheiben (Aluminium mit Schmelzpunkt 660°C oder Glas wird zähflüssig >1000°C) erreicht, ermöglichen gerade mal eine leichte Verformung. Ein Aufschrauben des Gehäuses und der Ausbau der Scheiben ist mindestens notwendig, um mit einem Lötbrenner an der Scheibe selbst höhere Temperaturen zu erzeugen. Ein Campinggas-Lötbrenner reicht dazu jedoch nicht aus. Ihr benötigt hierfür *Thermit*, ein Pulver, das in einer aus Ziegelsteinen improvisierten „Brennkammer" 2300°C heiß brennt und die Scheiben verflüssigt. Die Handhabung erfordert aller-

dings einige Vorsichtsmaßnahmen![29] Wem das zu viel Aufwand ist, der sollte zumindest die ausgebauten Scheiben der Festplatte in kleine Stücke brechen und an mehreren Orten verteilt entsorgen (Achtung - Splittergefahr!). Wegen der hohen Datendichte könnten Forensiker*innen darauf jedoch noch reichlich Datenfragmente finden! Alternativ könnt ihr die Oberfläche der einzelnen Scheiben mit einer Bohrmaschine und Drahtbürstenaufsatz abschleifen.

Flash-Speicher (USB-Sticks, SSD, SD-Karten, ...) lässt sich ebenfalls nur unvollständig zerstören. Mit zwei Zangen könnt ihr die Platine aus dem Gehäuse herausbrechen, um dann die Speicherchips samt Platine einzeln in Stücke zu brechen und in die Flamme eines Campinggas-Lötbrenner zu halten. Ihr erreicht auch hierbei nur eine partielle Zersetzung des Transistor-Materials. Vorsicht – Atemschutz oder Abstand! Die Dämpfe sind ungesund.

Optische Medien (CD, DVD, Blueray) lassen sich mit genügend großer Hitze vollständig und unwiderruflich zerstören. Das Trägermaterial Polycarbonat schmilzt bei 230°C (Deformation). Die Zersetzung gelingt bei 400°C und bei 520°C brennt es. Ein Campinggas-Lötbrenner reicht aus, die Scheiben aus Polycarbonat, einer dünnen Aluminiumschicht und einer Lackschicht zu Klump zu schmelzen oder gar zu verbrennen. Vorsicht – Atemschutz oder Abstand! Die Dämpfe sind ungesund. Alternative ist die Zerstörung des Datenträgers in der Mikrowelle (wenige Sekunden auf höchster Stufe)

Metadaten entfernen

Die meisten von euch kennen das Problem bei Fotos von Aktionen. Bevor diese veröffentlicht werden können, müssen nicht nur Gesichter unkenntlich gemacht werden[30], sondern auch die sogenannten Metadaten entfernt werden, die im Bild mit abgelegt sind und die Kamera, mit der das Bild aufgenommen wurde, eindeutig identifizieren. Neben der Uhrzeit und der Seriennummer sind bei einigen neueren Kameras (insbesondere Smartphones) sogar die GPS-Koordinaten in diesen sogenannten *EXIF*-Daten abgespeichert. Ein sogenanntes *Thumbnail* (Vorschau-Foto im Kleinformat) kann Bilddetails preisgeben, die ihr im eigentlichen Bild verpixelt oder anderweitig unkenntlich gemacht habt. Diese Metadaten müssen entfernt werden!

Leider tragen z.B. auch LibreOffice-/Worddokumente und PDF-Dateien Metadaten in sich. Anwender*innenname, Computer, Schriftarten, Namen und Verzeichnisorte eingebundener Bilder, … lassen Rückschlüsse auf euch bzw. euren Rechner zu.

Tails hat dazu eine umfassende Reinigungssoftware an Bord. Das **Metadata Anonymisation Toolkit** (**MAT**)[31] kann folgende Datentypen säubern: *PNG*- und *JPEG*-Bilder, *LibreOffice* und *Microsoft Office* Dokumente, *MP3* und *FLAC* (Audio-) Dateien und *TAR*-Archivdateien.

Anwendungen ▸ Systemwerkzeuge ▸ MAT (Metadata Anonymisation Toolkit)

Das Programm ist nahezu selbsterklärend:

Öffnet ein Dateimanager-Fenster, über das ihr die zu checkenden / säubernden Dateien hinzufügen könnt.

Überprüft, ob die angewählten Dateien sauber oder dreckig sind.

Die angewählten Dateien werden bereinigt und unter dem gleichen Namen wie die Originaldatei abgelegt. Ihr könnt dieses Werkzeug auch auf ganze Ordner anwenden. Bedenkt, dass die zusätzlich erzeugte Originaldatei mit dem Namens-Zusatz *.bak* auch nach dessen Löschen AUF DIESEM DATENTRÄGER immer noch rekonstruierbar ist!

Es hat sich herausgestellt, dass MAT Metadaten aus pdf-Dateien nicht zuverlässig entfernt. Aus diesem Grund unterstützt MAT das PDF-Format nicht mehr.

Zur Zeit wird die Entwicklung von MAT nur sporadisch fortgeführt. Der Entwickler empfiehlt, die Benutzung zu vermeiden und statt dessen auf andere Programme wie *exiftool* (umfangreiches Bereinigungstool), *exiv2* (löscht Metadaten aus Bildern), *jhead* (manipuliert Header in jpgs) oder *pdfparanoia* (bereinigt Wasserzeichen aus pdf-Dateien) zu benutzen. Leider wissen wir zur Zeit von keinem tool, das in der Lage ist, pdfs von allen Metadaten zu befreien. Grundsätzlich gilt:

> *Je größer das Sicherheitsbedürfnis, desto simpler sollte das Datenformat sein, das ihr für die Übermittlung wählt.*

Reines Textformat verrät am wenigsten über den Rechner, an dem der Text erstellt wurde. Beachtet, dass der *Name eines Dokuments* unter Umständen ebenfalls Rückschlüsse auf die Autor*in oder deren Rechner zulässt.

29 frank.geekheim.de/?p=2423

30 Zur Grafikbearbeitung könnt ihr das Programm GIMP verwenden.

31 https://mat.boum.org/

Mailen über Tor

Webmail

Die einfachste Methode in Tails Emails zu versenden und zu empfangen ist der Zugriff (über Tor) auf ein *Webmail-Konto*. Wurde das Mail-Konto anonym angelegt, lässt sich darüber die eigene *Identität* verschleiern. Andernfalls könnt ihr immerhin euren *Aufenthaltsort* verschleiern.

Für alle, die **verschlüsselten Mail-Text per Webmail** verschicken wollen, stellen wir im folgenden zwei Methoden der PGP-Verschlüsselung vor.

> *Warnung: Es ist unsicher, vertraulichen Text direkt in einen Webbrowser einzugeben, da Angreifer mit JavaScript aus dem Browser heraus darauf zugreifen können.*
>
> *Ihr solltet euren Text daher mit dem* **Tails OpenPGP Applet** *verschlüsseln und den verschlüsselten Text in das Browserfenster einfügen. Ihr müsst zusätzlich alle Skripte über NoScript verbieten!*

A) PGP-Verschlüsselung mit öffentlichem Schlüssel

Bei dieser Methode nutzt ihr die sehr sichere Standard-PGP-Verschlüsselung: Verschlüsseln mit den öffentlichen Schlüsseln der Empfänger*innen. Falls ihr noch nie mit PGP gearbeitet habt, könnt ihr Methode B) verwenden.

1. Schreibt euren Text in einen Texteditor, *nicht direkt in das Browserfenster eures Webmail-Anbieters!* Zum Beispiel könnt ihr dazu *gedit* öffnen über *Anwendungen ▸ Zubehör ▸ Texteditor* .

2. Markiert dort den zu verschlüsselnden oder zu signierenden Text mit der Maus. Um ihn in die Zwischenablage zu kopieren, klickt ihr mit der rechten Maustaste auf den markierten Text und wählt den Menüpunkt *Kopieren* aus. Das Tails OpenPGP Applet zeigt durch Textzeilen an, dass die Zwischenablage *unverschlüsselten Text* enthält.

3. Klickt auf das Tails *OpenPGP-Applet (in der Tails-Menüleiste oben rechts)* und wählt die Option **Zwischenablage mit öffentlichem Schlüssel signieren/verschlüsseln** aus. Sollte die Fehlermeldung *„Die Zwischenablage beinhaltet keine gültigen Eingabedaten"* angezeigt werden, versucht erneut den Text gemäß Schritt 2 zu kopieren.



4. Falls ihr den Text verschlüsseln wollt, wählt einen oder mehrere öffentliche Schlüssel für die Empfänger*innen des verschlüsselten Textes im *„Schlüssel wählen"*-Dialog aus *(siehe dazu das Kapitel PGP-Schlüssel importieren).*

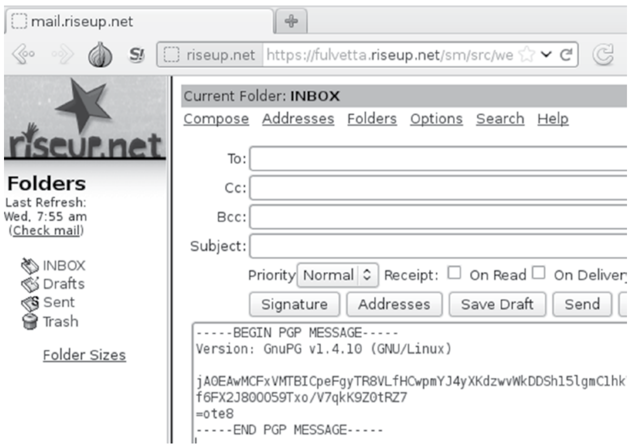
5. Falls ihr den Text signieren wollt, wählt den geheimen Schlüssel aus der *„Nachricht signieren als"*-Dropdown-Liste aus. Bedenkt, dass der Besitz dieses Schlüssels die Urheber*innenschaft der so signierten Mail schwer abstreitbar macht.

6. Klickt auf *OK*. Falls die Frage *„Vertrauen Sie diesen Schlüsseln?"* angezeigt wird, beantwortet dies entsprechend.

7. Falls ihr einen oder mehrere öffentliche Schlüssel zum Verschlüsseln des Texts ausgewählt habt, zeigt das Tails OpenPGP Applet durch ein *Vorhängeschloss* an, dass die Zwischenablage nun verschlüsselten Text enthält.
Habt ihr einen geheimen Schlüssel zum Signieren des Texts ausgewählt, so zeigt das Tails OpenPGP Applet nun durch ein *Siegel* an, dass die Zwischenablage signierten Text enthält.



8. Um den verschlüsselten oder signierten Text in das Webmail-Fenster eures Mail-Anbieters (oder eine andere Anwendung) einzufügen, klickt mit der *rechten Maustaste* auf das Eingabefeld, in das ihr den Text einfügen möchten, und wählt die Option *Einfügen* aus dem Menü aus.



B) PGP-Verschlüsselung mit Passphrase

Bei dieser Methode müsst ihr eine geheime Passphrase mit den Personen teilen, die die Nachricht entschlüsseln sollen. *Ihr müsst die Passphrase also zuvor über einen sicheren Kanal (im günstigsten Fall face-to-face) kommunizieren!*

Die beiden ersten Schritte sind identisch mit 1. und 2. aus Methode A). Dann geht es weiter mit:

1. ***Klickt auf das Tails OpenPGP Applet und wählt die Option* Zwischenablage mit Passwort verschlüsseln *aus. Sollte die Fehlermeldung* „Die Zwischenablage beinhaltet keine gültigen Eingabedaten“ *angezeigt werden, versucht erneut den Text gemäß Schritt 2 zu kopieren.***

2. ***Gebt eine Passphrase in den* Passphrase-*Dialog ein. Wiederholt die gleiche Passphrase im zweiten Dialog.***

3. ***Das Tails OpenPGP Applet zeigt durch ein Vorhängeschloss an, dass die Zwischenablage verschlüsselten Text enthält.***



4. ***Dieser Schritt ist identisch mit Schritt 8 aus Methode A).***

Entschlüsseln oder Signatur überprüfen

Die Entschlüsselung eines verschlüsselten Textes / einer verschlüsselten Mail funktioniert *für beide Verschlüsselungs-Methoden* folgendermaßen:

1. ***Markiert mit der Maus den verschlüsselten bzw. signierten Text (z.B. in eurem Webbrowser), den ihr entschlüsseln bzw. überprüfen möchtet. Schließt die Zeilen “-----BEGIN PGP MESSAGE-----“ und “-----END PGP MESSAGE-----” mit in die Markierung ein.***

2. ***Ist der ausgewählte Text verschlüsselt, zeigt dies das Tails OpenPGP Applet durch ein* Vorhängeschloss *an. Ist der ausgewählte Text nur signiert, aber nicht verschlüsselt, wird dies durch ein* Siegel *im Tails OpenPGP Applet angezeigt.***

3. ***Klickt auf das Tails OpenPGP Applet und wählt* Zwischenablage entschlüsseln/überprüfen *aus dem Menü aus.***

   - Ist der ausgewählte Text nur signiert und die Signatur gültig, erscheint direkt das GnuPG-Ergebnis Fenster.
   - Ist der Text signiert, aber die Signatur ungültig, wird das GnuPG-Fehler Fenster mit der Nachricht *„FALSCHE Unterschrift von...“* angezeigt. Ihr könnt euch nicht sicher sein, dass der angegebene Absender auch der tatsächliche ist.
   - Ist der Text **mit einer Passphrase** verschlüsselt, erscheint die Aufforderung *„Geben Sie die Passphrase ein...“*, danach auf „OK“ klicken.
   - Ist der Text *mit einem öffentlichen Schlüssel verschlüsselt* worden, können zwei verschiedene Dialoge angezeigt werden:
     - Ist die Passphrase zu einem geheimen Schlüssel noch nicht zwischengespeichert, dann erscheint ein Dialog mit der Nachricht: *„Sie benötigen eine Passphrase, um den geheimen Schlüssel zu entsperren“*. Gebt die Passphrase für diesen geheimen Schlüssel ein, danach auf *„OK“* klicken.
     - Falls sich kein zum verschlüsselten Text passender geheimer Schlüssel im Schlüsselbund befindet, wird die GnuPG Fehlermeldung *„Entschlüsselung fehlgeschlagen: Geheimer Schlüssel ist nicht vorhanden“* angezeigt.
   - Ist die Passphrase falsch, so wird ein *GnuPG-Fehler* Fenster mit der Meldung *„Entschlüsselung fehlgeschlagen: Falscher Schlüssel“* angezeigt.
   - Ist die Passphrase korrekt, oder ist die Signatur auf den Text gültig, so wird das *GnuPG-Ergebnis*-Fenster angezeigt.
   - **Der entschlüsselte Text erscheint im Textfeld Ausgabe von GnuPG.** Im Textfeld *Andere Nachrichten von GnuPG* zeigt die Nachricht *„Korrekte Unterschrift von...“* an, dass die Signatur gültig ist.

PGP-Schlüssel importieren

Da Tails über die aktuelle Sitzung hinaus keinerlei Daten speichert, müsst ihr für die Verschlüsselung mit Methode A bzw die Entschlüsselung zunächst einen PGP-Schlüssel von einem (hoffentlich verschlüsselten!) Datenträger importieren.

> ***Ihr solltet niemals private PGP-Schlüssel auf einem unverschlüsselten Datenträger speichern!***

Klickt dazu auf das Tails *OpenPGP-Applet (in der Tails-Menüleiste oben rechts)* und wählt die Option **Schlüssel verwalten.** Es öffnet sich die Passwort und Schlüsselverwaltung von Tails. Hier könnt ihr unter *Datei ► Importieren* einen verfügbaren Datenträger und dort den gewünschten Schlüssel auswählen. Beachtet, dass ihr zum **Entschlüsseln** *euren privaten PGP-Schlüssel* benötigt. Zum **Verschlüsseln** (mit Methode A) benötigt ihr hingegen den *öffentlichen Schlüssel des Empfängers*.

Ab jetzt stehen euch die so importierten PGP-Schlüssel bis zum Ende der Tails-Sitzung (also bist zum Herunterfahren des Rechners) zur Verfügung.

Remailer

Remailer ermöglichen das Versenden einer Mail z.B. an die Mail-Adresse einer Zeitungsredaktion ohne (zwingend) eine eigene Mailadresse anzugeben. Nur in Verbindung mit Tails und TOR bieten Remailer eine gute Möglichkeit, anonym Mails zu versenden. Dabei entstehen

teilweise beträchtliche Zeitverzögerungen, bis eine Mail die Empfänger*in erreicht.

Leider ist die Benutzung der von uns getesteten Remailer aktuell so umständlich, dass wir auf eine detaillierte Beschreibung verzichten müssen und auf die Website von *https://remailer.paranoici.org/* verweisen. Das in alten Versionen dieser Broschüre beschriebene Webinterface funktioniert derzeit nicht (mehr).

Chatten über Tor

Pidgin ist der Name des Chatclients, der bei Tails mitgeliefert wird. Im Vergleich zu einer Pidgininstallation unter einem „normalen" Linux ist das Pidgin von Tails speziell auf Verschlüsselung abzielend vorkonfiguriert.

Es wird nur eine limitierte Auswahl an Chatprotokollen angeboten: Varianten von *XMPP* und *IRC*. Für diese beiden Protokolle stehen Verschlüsselungsmethoden bereit, die anderen Protokollen fehlen. Die Voreinstellungen, die die Tails-Variante von Pidgin mitbringt, deaktivieren das *logging*, also das Mitprotokollieren von Sitzungen. Auch mitinstalliert ist das OTR-Plugin, welches eine Ende-zu-Ende-Verschlüsselung erlaubt[32].

Für den einmaligen Einsatz muss nichts weiter vorbereitet werden. Pidgin bei Tails kommt mit zwei vorkonfigurierten (zufälligen) Accounts daher, die direkt verwendet werden können. Für den regelmässigen Einsatz (mit eigenem Account) müsstet ihr Pidgin wegen der Vergesslichkeit von Tails jedes Mal neu konfigurieren oder die privaten Schlüssel auf einem Datenträger sichern.

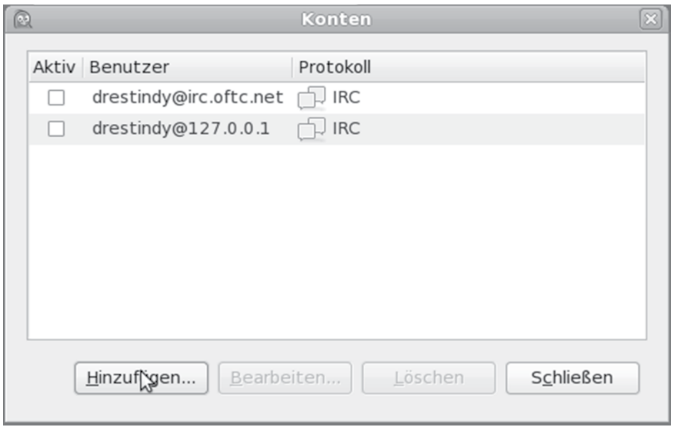
Pidgin findet sich unter *Anwendungen* ▸ *Internet* ▸ *Pidgin Internet-Sofortnachrichtendienst*.

Wenn Pidgin startet, zeigt es die sogenannte *Buddylist*, das ist so etwas wie ein Adressbuch. Nach dem ersten Start muss (mindestens) ein *Chat-Account* angelegt werden (das ist vergleichbar mit einer Email-Adresse) - es sei denn, ihr benutzt einen der beiden vorkonfigurierten Accounts.



Im Menü *Konten* ▸ *Konten verwalten* aufrufen. Zum Anlegen eines neuen Accounts auf „*Hinzufügen*" klicken. Hier die Daten des Chataccounts eintragen. Pidgin hat die Besonderheit, dass ein Chat-Account *name@jabber.server.org* getrennt eingetragen werden muss: „*name*" kommt in das Feld „*Benutzer*" und *jabber.server.org* in das Feld „*Domain*". Der Rest kann leer gelassen werden.

32 *OTR*: Off The Record – Ausdruck, der in Gesprächen signalisiert, dass das jetzt Gesagte nicht zitiert werden darf. Mehr zu OTR: https://otr.cypherpunks.ca/



Verschlüsselte Sitzung

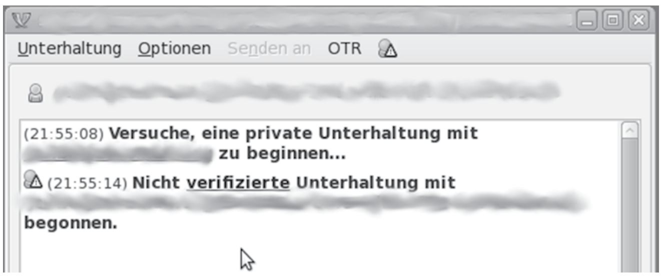
OTR verwendet das gleiche Schema wie auch PGP für seine Schlüssel: Es gibt einen öffentlichen und einen privaten.

Chatsitzungen von Pidgin sind beim Start nicht verschlüsselt – das Erste, was also (für jede Chatsitzung) gemacht werden muss, ist die „Private Unterhaltung" zu starten! Damit ist eine Ende-zu-Ende-Verschlüsselung via OTR gemeint.

Nach der Auswahl des Menüpunktes „*Private Unterhaltung*" startet eine verschlüsselte Sitzung.



Tippt sensible Inhalte erst nach dem Erscheinen der Meldung „*Unterhaltung mit ... begonnen*". Erst ab dieser Stelle wird alles, was in dieser Sitzung geschrieben wird, verschlüsselt übertragen.



Was auf dem Screenshot allerdings sichtbar wird, ist, dass das Gegenüber nicht verifiziert ist - sprich, **es ist nicht sicher, dass das Gegenüber die Person ist, für die sie sich ausgibt.**

Echtheit des Gegenübers verifizieren

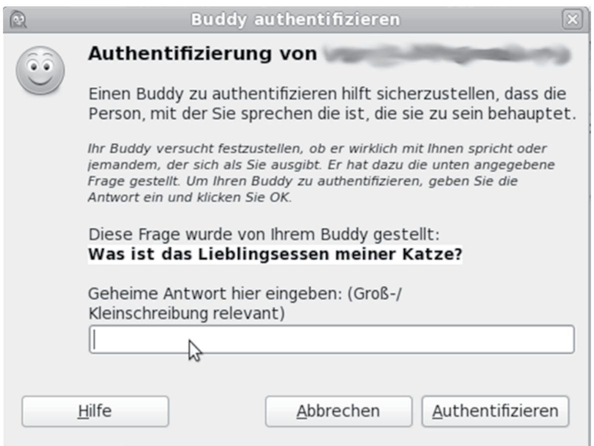


Um Zweifel auszuschließen, enthält Pidgin mehrere Methoden, um das Gegenüber zu identifizieren. **Es stehen drei Methoden zur Verfügung:**

- **Frage und Antwort:** Die Idee hinter dieser Methode ist, dass euer Gegenüber die Frage nur dann richtig beantworten kann, wenn sie die richtige Person ist. Fragen wie „Wie lautet mein Nachname" scheiden also aus, da die Antwort erraten werden kann. Vorteil dieser Methode ist, dass ihr euer Gegenüber nicht vorher getroffen haben müsst, um



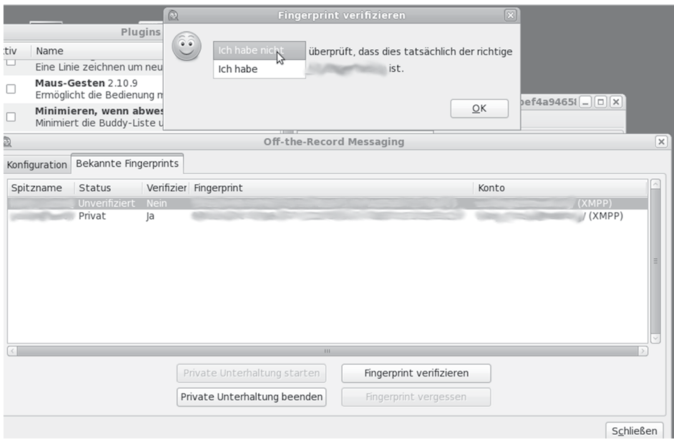
  ein entsprechendes Frage/Antwort-Paar vereinbart zu haben. Nachteil ist, dass eine entsprechende Frage mit nicht oder schwer erratbarer Antwort nicht leicht zu finden ist. Auf der anderen Seite sieht es dann so aus:



- **Gemeinsam bekannte Passphrase:** Einfacher ist es da schon, über einen sicheren Kanal ein gemeinsames „Passwort" oder gleich einen ganzen Satz zu vereinbaren. Dieser muss natürlich geheim bleiben.
- **Manueller Fingerprint-Vergleich:** Mit dieser Methode werden die öffentlichen Schlüssel direkt miteinander vergleichen - ihr habt den Fingerabdruck des öffentlichen Schlüssels eures Gegenübers und diese*r natürlich auch (ist ja ihr eigener). Sind die Abdrücke gleich, dann sind auch die öffentlichen Schlüssel gleich. Mit der Methode lässt sich ausschließen, dass jemand in der Mitte der Verbindung sitzt und beiden Seiten vorspielt, die jeweils andere Seite zu sein.

Am sichersten, aber wohl auch am umständlichsten, ist der *Fingerprint*-Vergleich. Die beiden anderen Verfahren haben entweder das Problem, ein gemeinsames Geheimnis sicher auszutauschen oder aber eine nicht erratbare Antwort auf eine Frage zu entwerfen. Von der Frage/Antwort-Variante raten wir also ab, es sei denn, diese sind über einen sicheren Kanal vereinbahrt worden.

Hier der Fingerprintvergleich als Screenshot, am Ende des Vergleichs wird das Ergebnis gespeichert, so dass der Vergleich nur einmal notwendig ist.



An dieser Stelle die Anmerkung, dass gespeicherte Fingerprints (ob überprüft oder nicht) ein Beleg für einen Kommunikationsvorgang sind und sich darüber ein Abbild eines soziales Netzes (wer kennt wenn, wer kommuniziert mit wem) ansammelt. Überlegt euch, ob es das wert ist - die Alternative wäre allerdings ein erneutes Überprüfen der Fingerprints bei jeder Sitzung, und wenn ihr die Schlüssel von OTR nicht speichert, sind auch die jedes mal neu mit entsprechend neuem Fingerprint.

Aktionsfotos bearbeiten

Bild öffnen

Ihr startet das Grafik-Programm *Gimp* unter *Anwendungen ► Grafik ► GNU Image Manipulation Program* und wählt euer Bild unter *Datei ► Öffnen* aus.

Bild skalieren

Heutige Digital-Kameras machen Fotos mit weit über zehn Megapixel Bildauflösung. Das kann für Plakate und Broschüren sinnvoll sein, ist aber für eine digitale Veröffentlichung z.B. bei *indymedia* oder eine Verschickung per Mail unnötig groß. Um das Bild kleiner zu machen, wählt ihr in *Gimp* die Funktion *Bild ► Bild skalieren*. Der Dialog zur Einstellung einer neuen Breite und Höhe ist selbsterklärend. Wenn ihr Breite und Höhe „verkettet" lasst, ändert sich das Seitenverhältnis des Bildes nicht. Eine Breite von z.B. 800 Pixel für ein Bild im Querformat ist für die meisten Internetzwecke ausreichend. Ihr beendet den Dialog mit dem Button *„Skalieren"*.

Bild-Bereiche unkenntlich machen

Ihr wählt im „Werkzeugkasten" das Werkzeug „Rechteckige Auswahl" und markiert einen Bereich, den ihr unkenntlich machen wollt. Der Bereich ist nun von einer laufenden gestrichelten Linie gerahmt. Ihr wählt *Filter ► Weichzeichnen ► Verpixeln* als eine Möglichkeit, den Informationsgehalt dieses Bildbereichs tatsächlich zu reduzieren. In der Vorschau seht ihr das verpixelte Ergebnis.

Ihr könnt die Pixelgröße einstellen und danach mit *„OK"* bestätigen. Mit der Wiederholung dieser Prozedur könnt ihr viele Bereiche (in denen z.B. Gesichter oder andere identifizierende Merkmale, wie z.B. Tatoos oder Schuhe zu sehen sind) unkenntlich machen.

Wenn ihr mit manchen Resultaten nicht zufrieden seid, lassen sich die Operationen Schritt für Schritt rückgängig machen mit der Funktion *Bearbeiten ► Rückgängig*.

Bild speichern

Dazu wählt ihr in *Gimp* die Funktion *Datei ► Exportieren* und gebt einen Namen für das zu speichernde Bild an (zum Beispiel *1.jpg*). Abhängig vom so gewählten Dateiformat (hier *jpg*) könnt ihr in diesem Dialogfenster noch die Qualität des zu speichernden Bildes beeinflussen (100 bedeutet keine Kompression, also hohe Detailgenauigkeit, aber auch größere Datei). Zum Abschluss klickt ihr auf *„Exportieren"*.

Beachtet, dass das bearbeitete Bild wie im Kapitel *„Metadaten entfernen"* beschrieben, bereinigt werden muss, um Metadaten wie z.B. die Kamera-Seriennummer und unverpixelte Vorschaubildchen zu entfernen!

Drucken

Zum Drucken den Drucker per USB-Kabel anschließen, anschalten und danach den Druckmanager unter *Anwendungen ► Systemwerkzeuge ► Einstellungen ► Drucker* starten. Dort „+" bzw „Neuen Drucker hinzufügen" auswählen und den (hoffentlich erkannten) Druckernamen mit *„Hinzufügen"* bestätigen.

Nun müsst ihr in der (lokal vorhandenen) Datenbank einen Druckertreiber finden. Dazu wählt ihr zunächst den Druckerhersteller und dann ein Modell, was eurem möglichst ähnlich ist. Häufig ist es ausreichend, das nächst ältere Modell samt dem vom Manager empfohlenen Treiber auszuwählen, falls ihr euer Druckermodell nicht findet. Ihr bestätigt die Wahl abschließend mit *„Anwenden"* und könnt eine *„Testseite drucken"*.

Hinweis: Ein eventuell schon vor der Druckerinstallation geöffnetes Programm (z.B. LibreOffice) muss erneut gestartet werden, um den „neuen" Drucker zu erkennen und für den Druck anzubieten.

Wer mehrfach den gleichen Drucker benutzt, kann sich die Installation am Anfang einer jeden Tails-Sitzung erleichtern, in dem er im Netz nach einem passenden Linux-Druckertreiber sucht. Die so heruntergeladene *.ppd-Datei* kann auf einem Datenstick dauerhaft gespeichert und anstelle der Suche in der lokalen Treiber-Datenbank angegeben werden.

Beachtet, dass ein Ausdruck über das spezifische Druckbild bei einer forensischen Untersuchung eindeutig einem einzelnen Drucker (nicht nur einem Druckertyp!) zugeordnet werden kann. Manche *Farbdrucker* hinterlassen zur Identifikation eine Kennung aus Einzelpunkten, die mit dem Auge nicht zu identifizieren ist[33]. Es handelt sich hierbei um unsichtbare Wasserzeichen, die einem Drucker eindeutig zugeordnet werden können *(machine identification code (mic))*.

Das bedeutet für eine sensible Print-Veröffentlichung, dass ihr preiswerte „Wegwerf"-Schwarzweiß-Drucker benutzen müsst. Wer durch anschließendes mehrfaches Kopieren (mit unterschiedlichen Kontraststufen) das Druckbild des Druckers verschleiern will, sollte beachten, dass fast alle Copy-Shops digitale Kopierer einsetzen, die mit einer großen Festplattenkapazität auch noch nach Wochen auf die einzelnen Druckaufträge inklusive exaktem Datum zugreifen können.

33 https://eff.org/issues/printers

Scannen

Zum Scannen den Scanner per USB-Kabel anschließen, anschalten und danach das Programm *„Simple Scan"* unter *Anwendungen* ► *Grafik* ► *Simple Scan* starten. Einfache (einseitige) Scanner funktionieren oft erst dann korrekt, wenn ihr im Programm unter *Dokument* ► *Einstellungen* ► *Scan Side* auf *„Front"* setzt. Falls gewünscht könnt ihr die Scan-Auflösung für Fotos bzw. Text verändern. Dann könnt ihr die Einstellungen *„Schließen"*. Achtet auch hier auf die Zuordenbarkeit zwischen Scan und Scanner.

Jetzt könnt ihr im Programm *Dokument* ► *Scannen* ► *Text /Foto* wählen, um anschließend mit dem Button *„Scannen"* eine Seite zu scannen. Falls die Einstellung Text zu keinem Ergebnis führt, schaltet auf die Einstellung Foto um. Ihr könnt die Seite(n) noch drehen oder auf einen bestimmten Bereich zuschneiden, bevor ihr das Dokument mit *„Speichern"* sichert.

Für eine weiterführende Nachbearbeitung des abgespeicherten Scans empfehlen wir das eben erwähnte Programm *Gimp*[34] .

Beamer benutzen

Wenn ihr in eurer Gruppe Dokumente gemeinsam diskutieren wollt, kann ein Beamer helfen. Falls euer Computer den Beamer nicht automatisch erkennt, müsst ihr in folgender Reihenfolge vorgehen: Den Beamer mit dem Computer verbinden, z.B. via VGA-Kabel oder HDMI-Kabel , einschalten und dann in Tails unter *Anwendungen* ► *Systemwerkzeuge* ► *Einstellungen* ► *Bildschirme* die Option *„Gleiches Bild auf allen Bildschirmen"* auswählen und bestätigen.

Falls euer Rechner den Beamer immer noch nicht als externen „Bildschirm" erkennt, könnt ihr euren Rechner mit einer der Funktionstasten[35] dazu bringen, das Bild auch an den VGA-Ausgang zu schicken. Mehrmaliges Drücken dieser Funktionstaste schaltet bei vielen Modellen zwischen den drei Einstellungen *„nur Laptop-Bildschirm"*, *„nur Beamer"* oder *„beide"* um.

34 siehe Kapitel *Aktionsfotos bearbeiten*

35 Welche Funktionstaste zum externen Bild umschaltet, hängt leider vom Rechner-Hersteller ab, ist aber als Symbol auf der Tastatur erkennbar.

Warnung: Grenzen von Tails

Wir stellen hier einige Warnungen zur Nutzung von Tails und Tor zusammen, die ihr zur Bewertung eurer Sicherheit und zur Überprüfung nutzen könnt, in welchem Umfang Tails für eure spezifischen Anforderungen geeignet ist[36].

Tails verschlüsselt *nicht automatisch* eure Dokumente, löscht *nicht automatisch* die Metadaten aus euren Dokumenten und verschlüsselt auch keine Mail-Header eurer verschlüsselten Mails!

Tails nimmt euch auch nicht die Arbeit ab, eure Netzaktivitäten (entlang tätigkeitsbezogener Identitäten) aufzutrennen, und Tails macht schwache Passwörter[37] nicht sicherer.

Kurzum, Tails ist kein Wunderheilmittel für Computer-Nicht-Expert*innen. Ihr müsst also grob verstehen, was ihr (mit Hilfe von Tails) macht und ihr müsst euer Netzverhalten neu entwerfen (siehe Kapitel *Nur über Tor ins Netz*).

Ihr könnt nicht verschleiern, dass ihr *Tor* und Tails verwendet

Tor-Nutzer*innen sind als solche erkennbar – folglich auch die Nutzer*innen von Tails, denn Tails schickt automatisch alle Verbindungen über das *Tor*-Netzwerk. Der Zielserver (z.B. die Webseite, die ihr besucht) kann leicht feststellen, dass ihr *Tor* nutzt, da die Liste der *Tor*-Exit-Rechner **3** (siehe Kapitel *Nur über Tor ins Netz*) für alle einsehbar ist.

Tails versucht es so schwer wie möglich zu machen, *Tails*-Nutzer*innen von *anderen Tor*-Nutzer*innen abzugrenzen, insbesondere von Nutzer*innen des *Tor Browser Bundles* .

Manche Webseiten fragen viele Informationen über die Browser der Besucher*innen ab. Zu den gesammelten Informationen können unter anderem Name und Version des Browsers, die Fenstergröße, eine Liste mit den verfügbaren Erweiterungen und Schriftarten sowie die Zeitzone gehören. Einige dieser Merkmale können z.B. über die Nutzung von *NoScript*[38] im *Tor*-Browser unterdrückt werden. Andere, wie z.B. die Bildschirmauflösung und die Farbtiefe können unseres Wissens nicht unterdrückt werden. Diese Kennungen können eine Identifikation des Rechners erleichtern, bzw. eine Zuordnung eures Aufrufes einer Webseite zu anderen bereits besuchten Webseiten ermöglichen[39].

36 https://tails.boum.org/doc/about/warning/index.de.html

37 siehe dazu das Kapitel *Sichere Passwortwahl*

38 siehe dazu das Kapitel *Surfen über Tor*

39 http://heise.de/-1982976

Tor schützt nicht vor einem globalen Angreifer

Wie sicher ist die Verschleierung der IP-Adresse bei Benutzung des Tor-Netzwerks? Ergänzend zum Kapitel „*Ist Tor noch sicher?*" in der Einführung hier noch einige Anmerkungen.

Ihr könnt in jedem Fall enttarnt werden, wenn ihr es mit einem *globalen Angreifer* zu tun habt, das heißt, wenn jemand alle Rechner des Tor-Netzwerks korrumpiert hat bzw. den Datenverkehr zwischen allen Tor-Rechnern in Echtzeit mitprotokolliert. Einem solchen Angreifer ist es möglich, über die Analyse von Zeitstempeln und Größe der ausgetauschten (verschlüsselten) Datenpakete einzelne Tor-Nutzer*innen den jeweiligen Zielservern zuzuordnen – also die Anonymität aufzuheben![40]

Jeder Mensch weltweit mit einem Netzanschluss genügend großer Bandbreite kann seinen Rechner dem Tor-Netzwerk zur Verfügung stellen – auch Behörden und andere verdeckte Angreifer. Verteilt über die ganze Welt beteiligen sich derzeit über 7000 Rechner von verschiedenen Institutionen und Privatmenschen am Tor-Netzwerk.

Eine im Oktober 2013 veröffentlichte Studie von Wissenschaftler*innen[41] befasste sich mit dem bereits bekannten Problem der ausgedehnten Protokollierung des Tor-Netzwerkverkehrs. Ziel war es, die Wahrscheinlichkeit und den Zeitraum einschätzen zu können, der benötigt wird, um genügend Daten (über Alltagsroutinen im Netz) für eine Zerstörung der Anonymität zu sammeln. Nach dem dort untersuchten Modell könnte in sechs Monaten durch den Betrieb eines einzigen Tor-Rechners, die Anonymität von 80% der verfolgten Benutzer*innen durch gezielte Suche nach wiederkehrenden Traffic-Mustern gebrochen werden.

Die Praxis schien zumindest *zum Zeitpunkt der von Snowden kopierten Geheimdokumente* (im Frühjahr 2013) etwas komplizierter als derartige Modelle. Ein Artikel der britischen Zeitung *The Guardian* berichtete im Herbst 2013 von geringen Erfolgen, welche die NSA beim Versuch verbuchte, Tor-Benutzer*innen zu identifizieren. Zugrunde lagen dem Artikel die Snowden-Dokumente über *Prism*. „Wir werden niemals alle Tor-Nutzer identifizieren können", zitierte der Guardian aus einer Top-Secret-Präsentation mit dem Titel „*Tor* stinks". Mit manueller Analyse sei man *(damals)* lediglich in der Lage (gewesen), einen sehr kleinen Anteil der Tor-Nutzer*innen zu identifizieren. Insbesondere habe die Agency bislang keinen Erfolg damit gehabt, Anwender*innen auf konkrete Anfragen hin gezielt zu de-anonymisieren.

Die bislang veröffentlichten „Enttarnungserfolge" beruhten auf (noch nicht geschlossenen) Sicherheitslücken des verwendeten Browsers und insbesondere der installierten Browser-Plugins(!), auf Anwendungsfehlern oder auf immer gleichen Mustern der Nutzer*innen.

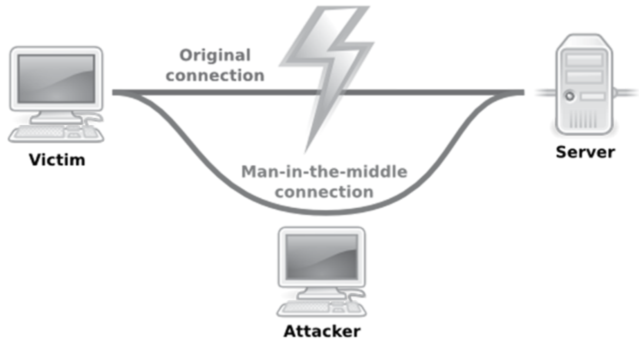
VRAM Analyse

Bei einer nicht weiter bekannten Anzahl von verbreiteten Grafikkarten kann ein Angreifer die im Arbeitsspeicher der Grafikkarte (VRAM) hinterlegten Bildschirmdaten wiederherstellen. Tails bietet aktuell (in Version 2.3) keine Möglichkeit dies zu unterbinden. Die Wiederherstellung von Bildschirmdaten, die unter dem Namen „Palinopsie Bug" bekannt wurde, betrifft auch virtuelle Umgebungen wie Virtualbox. Davon betroffen sind mehrere ATI- und NVIDIA Grafikkarten[42].

Man-in-the-middle-Angriffe

Bei einer solchen Attacke greift ein *Man-in-the-middle* aktiv in die Verbindung von eurem Rechner zu einem Zielserver ein: Ihr denkt, dass ihr direkt mit dem Server eures Mail-Anbieters oder mit der Eingabemaske des Nachrichten-Portals de.indymedia.org verbunden seid, tatsächlich sprecht ihr mit der Angreifer*in, die das eigentliche Ziel imitiert[43].

Auch bei der Benutzung von Tor sind derartige Angriffe möglich - sogar Tor-Exit-Rechner[44] können solche Angreifer sein[45]. Eine verschlüsselte Verbindung (SSL-Verschlüsselung für euch im Browser am https://... erkennbar) ist hilfreich, aber nur dann, wenn ihr die Echtheit des *Zertifikats einer solchen Verbindung überprüfen* könnt.



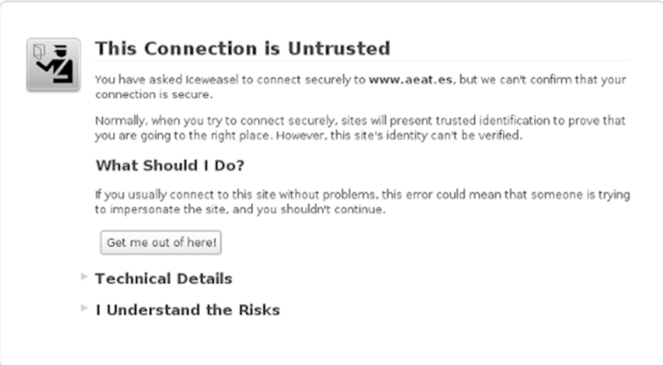
Wir gehen hier nicht tiefer auf Zertifizierungsmethoden

40 Wer mehr über die Zielsetzung und das Bauprinzip von Tor erfahren will: Tor Project: The Second-Generation Onion Router (Kapitel 3, Design goals and assumptions) https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf
41 http://www.ohmygodel.com/publications/usersrouted-ccs13.pdf

42 https://hsmr.cc/palinopsia/
43 Die NSA geht hier noch einen Schritt weiter und erweitert Man-in-the-middle-Angriffe durch Man-on-the-side-Angriffe: Diese Variante hat den „Vorteil", dass keine Verzögerungen im Datenverkehr wahrgenommen werden. Siehe dazu: https://en.wikipedia.org/wiki/Man-on-the-side_attack
44 siehe zur Funktionsweise von Tor das Kapitel Nur über Tor ins Netz
45 Man-in-the-middle Angriffe von Tor-Exit-Rechnern ausgeführt: https://www.heise.de/security/meldung/Anonymisierungsnetz-Tor-abgephisht-Teil-2-197888.html

und deren Verlässlichkeit ein, wollen euch aber zumindest die Basis für ein gesundes Misstrauen mitgeben:

Wenn euch dieser Bildschirm beim Verbindungsaufbau angezeigt wird, dann konnte die *Echtheit eures Zielservers* (in unserem Beispiel der Mailanbieter oder indymedia) nicht garantiert werden. Damit ist nicht gesagt, dass an der Verbindung wirklich etwas „faul“ ist.



Wenn ihr jedoch die Möglichkeit habt, den unter „*Technical Details*“ angezeigten (vorgeblichen) *Fingerprint* eures Zielservers zu überprüfen (Besuch der Seite von einem anderen Rechner aus, oder andere Quellen), dann solltet ihr das tun!

Das wehrt nicht alle Arten von Man-in-the-Middle-Attacken ab, erschlägt aber einen großen Anteil.

Tails unterstützt euch mit dem Tor-Browser-Plugin** HTTPS-Everywhere **dabei, (wo möglich) SSL-verschlüsselte Verbindungen aufzubauen. Wenn ihr die Möglichkeit habt, die Echtheit dieser Verbindung über den** Fingerprint **zu überprüfen, solltet ihr das unbedingt tun.

Cold-Boot Angriffe

Bei der Benutzung eines Computers werden alle bearbeiteten Daten temporär im Arbeitsspeicher zwischengespeichert - auch Passwörter und PGP-Schlüssel!

Nachdem ihr den Computer ausschaltet, geht der Inhalt des Arbeitsspeichers nicht sofort, sondern (je nach Temperatur[46]) erst *nach einigen Minuten* verloren. Angreifer*innen können diese Zeit zum Auslesen des Arbeitsspeichers nutzen, benötigen dazu jedoch physischen Zugang zum Rechner.

Tails überschreibt beim Herunterfahren bzw. Ausschalten des Rechners (per Power-Off) Teile des Arbeitsspeicher deswegen mit Zufallszahlen. Das klappt jedoch nicht bei allen Computern: Wenn sich euer Rechner beim Herunterfahren oder beim „Ausschalten“ nach zwei Minuten nicht selbstständig ausschaltet, dann gibt es keine Garantie dafür, dass das Überschreiben (vollständig) funktioniert hat.

Im Fall einer überraschenden Beschlagnahmung eures Rechners sofort den Ausschalter drücken! Es ist ratsam, den Rechner herunterzufahren, wenn er längere Zeit unbeaufsichtigt ist - z.B. in der Nacht.

Keylogger

Wenn ihr einen nicht vertrauenswürdigen Computer verwendet, z.B. einen für alle zugänglichen in einer öffentlichen Bibliothek, dann kann potentiell alles, was ihr über die Tastatur eingebt, von einem *Hardware Keylogger* aufgezeichnet werden.

Um die Eingabe von Passwörtern oder sensiblen Texten vor einem Keylogger zu schützen, könnt ihr die *Bildschirmtastatur* verwenden. Um die Bildschirmtastatur anzuzeigen, klickt ihr auf das **Tastatursymbol in der Kontrollleiste oben**. Jeder Klick auf dieser *virtuellen* Tastatur ersetzt dann einen *realen* Tastaturanschlag. Da auch das Fernauslesen des Bildschirminhalts nachweislich zu den Angriffsmethoden der Geheimdienste gehört, raten wir grundsätzlich:

Wenn ihr der Hardware nicht trauen könnt, benutzt sie nicht für sensible Arbeit!

Gefahren von kabellosen Schnittstellen

Beim Start von Tails werden die kabellosen Schnittstellen **WLAN, wwan, wimax, bluetooth** *- sofern in eurem Computer vorhanden - (mit geänderter MAC-Adresse)* **aktiviert.**

Beim **WLAN** reicht die Manipulation der MAC-Adresse aus, um von anderen Geräten in Reichweite *falsch* identifiziert zu werden.

Die **Bluetooth**-Schnittstelle eures Laptops hingegen benutzt zur Identifikation nicht nur eine der MAC ähnliche Adresse, sondern auch eine andere, nicht veränderbare Geräte-Adresse[47]. Das heißt aber: **Euer Laptop kann von anderen Geräten mit einer Bluetooth-Schnittstelle identifiziert werden – je nach Übertragungsstandard bis zu 100 Meter weit[48]!**

---

46 Je kälter, desto länger „hält sich“ der Speicherinhalt. Daher benutzen Forensiker zur Datenwiederherstellung beschlagnahmter Geräte Kältemittel zur kurzfristigen „Daten-Konservierung“.

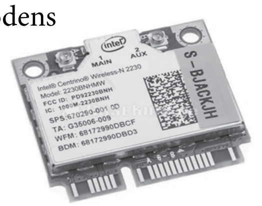
47 Die Situation ist ähnlich dem im Kapitel *Tails ändert eure MAC-Adressen* beschriebenen Problem mit den UMTS-Sticks, die zur Anmeldung beim Mobilfunk-Anbieter zusätzlich die IMSI der SIM-Karte und die IMEI des Sticks übermitteln.

48 *Die häufigsten Bluetooth-Geräte (der Klasse 2) haben mit einer Sen-*

Daher ist es für eine sichere Betriebsart von Tails unerlässlich, sämtliche nicht benötigte Funkschnittstellen abzuschalten. Wir beschreiben hier drei unterschiedliche Methoden. Wir halten Variante 1 für die sicherste:



1. **Bluetooth[49] ausbauen**
   In vielen neueren Laptops findet sich *eine Karte*, die sowohl das WLAN, als auch das Bluetooth-Modul beinhaltet (siehe Abbildung rechts). Nach Lösen aller Schrauben des Laptop-Bodens und dem Abnehmen des Bodendeckels könnt ihr die beiden Antennenanschlüsse abziehen und die Karte(n) herausnehmen. Im Falle einer kombinierten Bluetooth/WLAN-Karte[50] müsst ihr diese durch eine reine WLAN-Karte ersetzen.



2. **Bluetooth im BIOS deaktivieren**
   Dies ist leider nicht bei allen Computern möglich.
3. **Softwareseitig abschalten**
   Solange Tails in seinem Startbildschirm *nicht* die Option anbietet, Bluetooth und andere Funkschnittstellen vor Systemstart zu deaktivieren, müsst ihr einen umständlichen *Workaround* nutzen: An einem für euch untypischen Ort Tails starten, dann alle Geräte in Tails manuell deaktivieren und danach einen **Ortswechsel** vornehmen, um woanders mit der Arbeit zu beginnen. Dazu müsst ihr:
   - Beim Startbildschirm *„weitere Optionen"* wählen und ein *Administrator-Passwort* eingeben[51].
   - Nach dem Start *Anwendungen* ► *Zubehör* ► *Root Terminal* anklicken. Jetzt werdet ihr nach dem zuvor eingegebenen Administrator-Passwort gefragt. Bei richtiger Eingabe öffnet sich ein so genanntes Terminal, in dem ihr folgende Befehlssequenz eintippt und mit der *Eingabe-Taste* abschickt:
   - **rfkill block bluetooth wimax wwan**[52]

Fertig - jetzt könnt ihr an den *Ort wechseln*, an dem ihr per WLAN ins Netz gehen wollt. **Achtet darauf, dass der Rechner während des Ortswechsels nicht ausgeht!**

Bei der (unsichersten) Variante 3 habt ihr das Problem jedoch lediglich software-technisch auf Betriebssystem-Ebene gelöst. Eine eventuell während der Sitzung eingeschleuste Schadsoftware kann eben diese Deaktivierung aller Funkschnittstellen mit einem weiteren Kommando genauso einfach rückgängig machen.



Tails als Quasi-Schreibmaschine

Im Februar 2015 veröffentlicht der Antiviren-Software-Hersteller *Kaspersky,* dass die NSA in größerem Umfang die Firmware von Festplatten infiziert. Die eingeschleuste Schadsoftware überlebt eine Formatierung der Festplatte oder Neuinstallation des Betriebssystems und sei nicht zu entdecken. Gleichzeitig werde sie genutzt, um einen versteckten Bereich auf der Festplatte zu schaffen, auf dem Daten gesichert werden, um sie später abgreifen zu können. Die einzige Möglichkeit, die Schadsoftware loszuwerden sei die physikalische Zerstörung der Festplatte.

Für eine sicheres, spurenfreies Bearbeiten von extrem sensiblen Dokumenten empfehlen wir die Arbeit an einem Rechner, der weitgehend abgeschottet ist und insbesondere keine Festplatte(n) besitzt.

Festplatte(n) abschalten

Zwar müsstet ihr die im Computer vorhandene Festplatte wie jeden anderen Datenträger auch in Tails erst im Menü *Orte* ► *Rechner* verfügbar machen, bevor ihr (versehentlich) darauf etwas speichern könnt. Aber genau solche „Versehen" und die Möglichkeit, dass eine in der Sitzung eingeschleuste Schadsoftware doch auf die Festplatte zugreifen könnte, wollen wir ausschalten. Wir stellen euch zwei Methoden vor. Wir empfehlen die erste:

- **Festplatte ausbauen**
  In der Bedienungsanleitung *(ansonsten User Manual im Internet suchen)* eures Rechners sind die dazu notwendigen Schritte erläutert. Als erstes müsst ihr den Akku aus eurem Laptop herausnehmen und den Netzstecker abziehen. *Bei vielen Laptops* müsst ihr die Schrauben auf dem Boden lösen und den Boden abnehmen. Die Festplatte ist mit dem Restgehäuse zusätzlich verschraubt. Nachdem ihr diese gelöst habt, könnt ihr die Festplatte vom Stecker abziehen.
- **Festplatte im BIOS deaktivieren**
  Wenn euch der Ausbau zu aufwändig erscheint,

---

deleistung von 2,5 mW etwa 10m Reichweite. Im Freien können sie aber aus bis zu 50 Metern Entfernung noch erkannt werden! Die selteneren Geräte der Klasse 1 können eine Reichweite drinnen und draußen von 100 Metern erreichen, benötigen dafür aber auch 100 mW. Gegenwärtig liegen Geräte mit Bluetooth der Klasse 3 im Trend. Mit einer Leistungsaufnahme von 1 mW sind sie nur für den Einsatz bei kurzen Strecken und in Geräten mit langer Akkulaufzeit gedacht, wie etwa Headsets, Hörgeräten oder Pulsmessern, die beispielsweise ihre Daten an Smartphones weitergeben. Durchschnittlich liegt deren Reichweite bei etwa einem Meter, maximal sind es zehn.

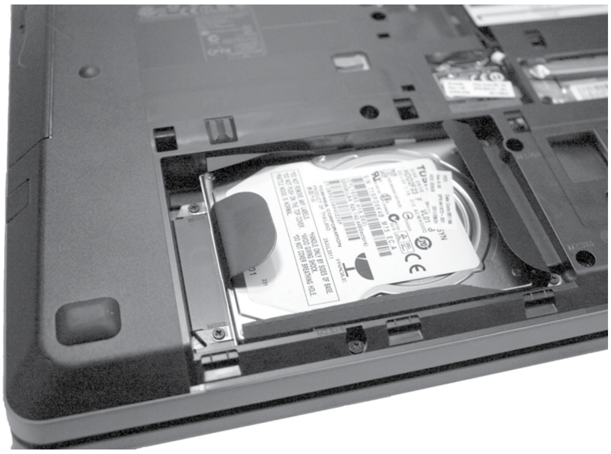
49 Da die Bauart dieser Karten und die Orte wo (im Rechner) genau sie verbaut sind, variieren, müsst ihr in der Betriebsanleitung (User Manual) eures Computers nach einer Beschreibung zu deren Ein-und Ausbau suchen.

50 siehe dazu das Kapitel *Tails als Quasi-Schreibmaschine*.

51 Siehe dazu das Kapitel *„Tails starten"*

52 mit **rfkill block bluetooth** bzw. **rfkill block wlan** lassen sich die Schnittstellen auch einzeln abschalten, falls ihr die jeweils andere benötigt.

müsst ihr zumindest im BIOS die interne(n) Festplatte(n) eures Computers deaktivieren[53].



Alle kabellosen Schnittstellen abschalten

Das kabelgebundene Netz (LAN) lässt sich einfach über das Abziehen des Netzwerkkabels „deaktivieren“. Zusätzlich ist es für diese besonders sichere Betriebsart von Tails als „Quasi-Schreibmaschine“ unerlässlich, sämtliche Funkschnittstellen abzuschalten. Wir beschreiben hier drei unterschiedliche Methoden *(1 ist die sicherste, 3 die unsicherste)*:

1. **WLAN und Bluetooth[54]ausbauen**
   analog zu Schritt 1 im vorherigen Kapitel Gefahren von kabellosen Schnittstellen. Ihr ersetzt die ausgebaute Karte jedoch nicht.

2. **Alle Netzwerkadapter im BIOS deaktivieren *(leider nicht bei allen Computern möglich).***

3. ***Ihr startet Tails neu und wählt am Startbildschirm „weitere Optionen“, um dann* „Alle Netzwerkfunktionen deaktivieren“ anzuklicken.**
   Hiermit bleiben (seit Version Tails-1.8) alle Netzwerkadapter softwareseitig beim Start deaktiviert. Dies geschieht sinnvoller Weise *bevor* Tails seine Netzwerkfunktionalität startet. So bleiben u.a. WLAN und Bluetooth still und können eure Anwesenheit in Funkreichweite anderer Geräte nicht mehr preisgeben.

53 Unmittelbar nach dem Computer-Start eine der Tasten F1, F2, DEL, ESC, F10 oder F12 gedrückt halten (auf einen Hinweis auf dem *kurz* erscheinenden Startbildschirm achten), um in das BIOS-Setup zu gelangen. Siehe dazu das Kapitel im Anhang: „Bootreihenfolge im Bios ändern“.

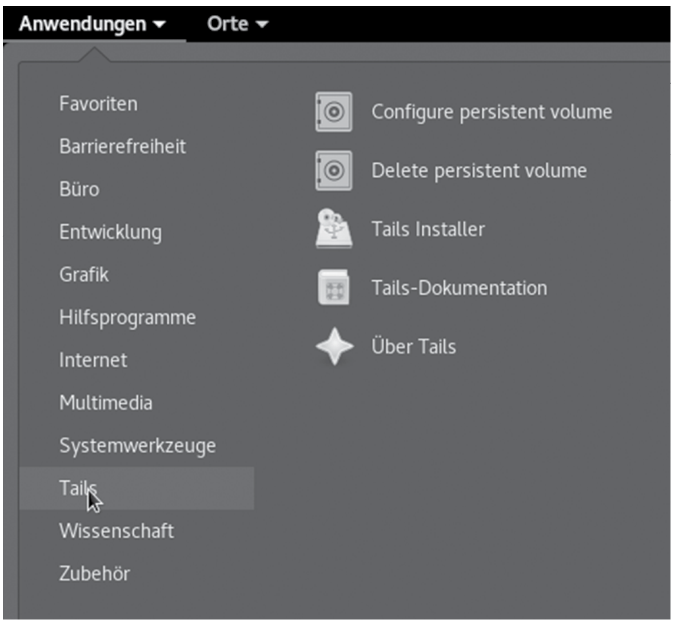
54 Da die Bauart dieser Karten und die Orte wo (im Rechner) genau sie verbaut sind, variieren, müsst ihr in der Betriebsanleitung (User Manual) eures Computers nach einer Beschreibung zu deren Ein-und Ausbau suchen. Hier ein Abbild einer kombinierten WLAN- und Bluetooth-Karte eines Laptops.

Ein vollständig abgeschotteter *Schreib-Computer,* ***aus dem ihr die Festplatte(n) und alle kabellosen Netzwerkadapter ausbaut, gibt euch erhöhte Sicherheit beim Erstellen und Bearbeiten von Dokumenten: Ihr seid ohne weiteres nicht zu identifizieren und zu lokalisieren und ihr verhindert ein „versehentliches“ Speichern auf Festplatte!***

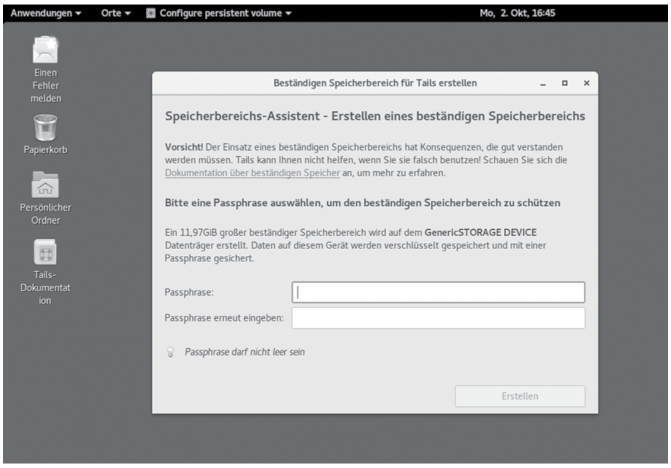
Persistenz

Daten und Einstellungen bleiben auf dem Tails-USB-Stick erhalten.

Bei normaler Benutzung werden alle Daten und alle Einstellungsänderungen (gespeicherte Texte, Bilder, Verschlüsselungskeys, Programmkonfigurationen, etc.) mit dem Runterfahren des Rechners verworfen. Das hat den Vorteil, dass keine individuellen Spuren auf dem Stick verbleiben, schränkt aber die bequeme Benutzbarkeit für einige Anwendungen ein. Um dem zu begegnen, gibt es bei der Nutzung von Tails auf einem USB-Stick die Möglichkeit, ein sogenanntes *“persistent volume”* zu verwenden. Gemeint ist damit ein Speicherbereich auf dem Tails-Stick, welcher eben nicht vergesslich ist. Dieser Speicherbereich wird von dem Platz auf dem USB-Stick abgezweigt, der nicht von der Tails-Installation (etwa 1,3 GB) belegt wird. Je mehr Kapazität also der USB-Stick hat, um so größer fällt das *“persistente Volume”* aus.

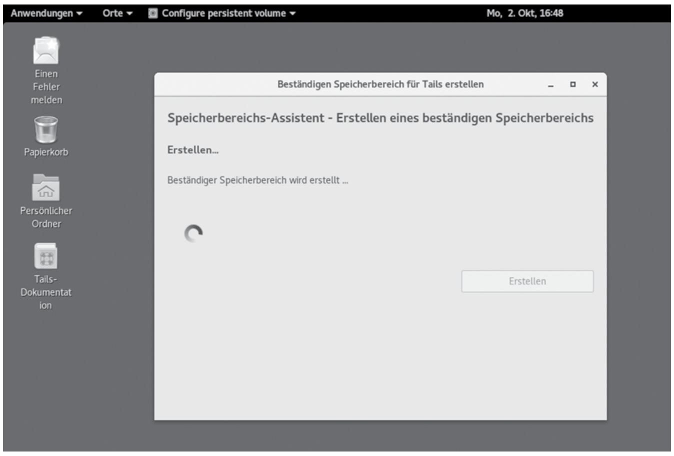


Es erscheint ein Dialog mit Hinweisen und der Abfrage des Passworts. Bitte beachtet die Hinweise in dieser Broschüre zur Auswahl eines starken Passworts.

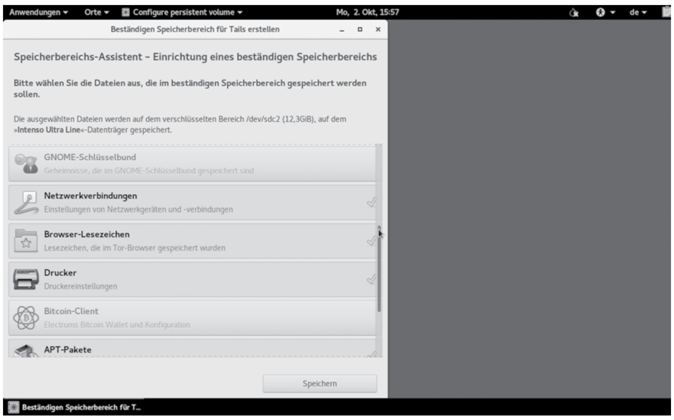


Nach Eingabe des Passwortes wird das persistente Volume erzeugt, was einen Moment dauern kann.

Ist dieser Vorgang abgeschlossen, folgt der Dialog zu Konfiguration des *persistent Volume*. Ihr könnt übrigens



diese Konfiguration zu jedem späteren Zeitpunkt anpassen. Eine Erklärung des Konfigurationsdialogs:



* **Persönliche Daten:** In eurem Home-Verzeichnis wird ein Ordner “Persistent” erzeugt. Dokumente (Bilder, Texte, etc.) die in diesem Ordner liegen, “überleben” einen reboot von Tails und sind in der nächsten Sitzung immer noch vorhanden.

* **GnuPG:** Öffentliche und private GPG/PGP Schlüssel bleiben erhalten.

* **SSH-Programm:** Benutzt man diese Funktion, bleibt Schlüsselmaterial des SSH-Programms erhalten.

* **Pidgin:** Auch das Chat-Programm Pidgin verwendet Schlüssel, um eine sichere Kommunikation zu erlauben. Sollen diese Schlüssel erhalten bleiben, dann aktiviert diesen Punkt. Mehr dazu im Kapitel *Chatten über Tor*.

* **Thunderbird:** Tails bringt ein E-Mailprogramm mit, dessen Einstellungen (Mailserver, Accountdaten, etc.), aber auch heruntergeladene Mails bleiben erhalten, wenn dieser Punkt aktiviert ist. Mehr dazu im Kapitel *Mailen mit Persistenz.*

* **Gnome Schlüsselbund:** Tails benutzt einen Keymanager, der dafür sorgt, dass Passwörter, die ihr für einen Dienst eingebt, nicht nochmal eingegeben werden müssen, wenn ihr diesen Dienst ein zweites Mal verwendet – das GPG-Passwort ist ein Beispiel dafür: Einmal eingegeben wird es bei der nächsten verschlüsselten Mail wieder verwendet. Aktiviert ihr diesen Punkt, dann bleiben diese Passwörter auf dem Stick gespeichert. Wir raten von der Benutzung ausdrücklich ab!

* **Netzwerkverbindungen:** Habt ihr spezielle Netzwerkkonfigurationen (z.B. UMTS-Sticks), ohne die ihr nicht ins Internet kommt, dann könnt ihr die durch Aktivierung dieses Punktes haltbar machen.

* **Browser-Lesezeichen:** Aktiviert ihr diesen Punkt, dann bleiben die Bookmarks erhalten.

* **Drucker:** Eure Druckerkonfiguration bleibt erhalten.

* **APT-Pakete:** Habt ihr auf dem Tails Stick eigene Software installiert, so ist diese normalerweise nach einem Reboot verschwunden. Aktiviert ihr diesem Punkt, bleibt sie erhalten.

* **APT-Listen:** APT ist eine oder besser die Softwareverwaltung von Debian, aus welchem Tails besteht. APT pflegt Listen von Softwarepaketen, die installierbar sind inklusive der Versionsnummern, so dass veraltete Pakete erkannt werden. Wenn ihr eigene Software installiert, dann aktiviert auch diesen Punkt.

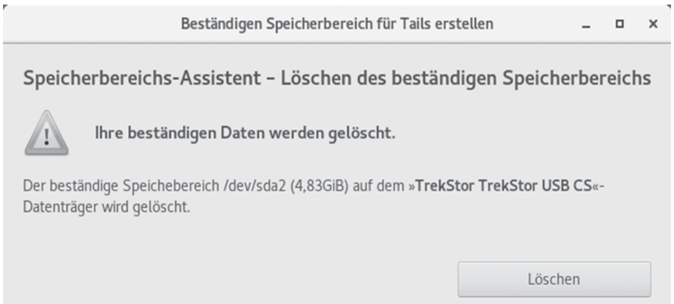
* **Punktdateien:** Tails bringt eine Menge Programme mit. Passt ihr deren Konfiguration an, dann werden diese in sogenannte Punktdateien (dot-files) gespeichert. Aktiviert diesen Punkt, wenn ihr eure individuellen Anpassungen behalten wollt und diese nicht durch die oben genannten Punkte bereits abgedeckt sind.

Anpassen und Löschen des Persistent Volume

Den oben beschriebenen Konfigurationsdialog bekommt ihr unter *Anwendungen* ►*Tails* ►*Configure persistent Volume.*

Solltet ihr euer persistent Volume löschen wollen, dann wählt *Anwendungen* ► *Tails* ► *Delete persistent Volume.*

Wenn ihr jetzt auf *"Löschen"* klickt, sind die Daten in dem persistenten Volume unwiederbringlich weg! Ihr könnt zu einem späteren Zeitpunkt die ganze Prozedur wiederholen, um ein neues persistentes Volume zu erzeugen.



Benutzung des Persistent Volume

Damit ihr das Persistent Volume benutzen könnt, müsst ihr rebooten. Im Anfangsdialog werdet ihr gefragt, ob ihr das Persistent Volume benutzen wollt. Bejaht das und gebt das Passwort ein. Fertig.

Daten von Hand vom Persistent Volume auf ein anderes Speichermedium kopieren

Falls ein Upgrade auf eine neue Tails-Version Probleme bereitet und ihr manuell einen neuen (anderen) Tails-Stick erzeugt, dann müssen eure Einstellungsdateien und eure Daten auf den persistenten Speicherbereich des neuen Sticks kopiert werden. Wir beschreiben hier, wie das geht:

Sichern der Dateien vom alten Tails-Medium:

1. Schließt das alte Tails-Medium an, von welchem ihr eure Daten sichern möchtet.

2. Wählt *Anwendungen* ► *Hilfsprogramme* ► *Laufwerke.*

3. Wählt im linken Fensterbereich das Medium aus, welches dem alten Tails-Medium entspricht.

4. Wählt im rechten Fensterbereich die Partition mit dem Typ LUKS aus. Der Name der Partition muss *TailsData* lauten.

5. Klickt auf die Schaltfläche *Entsperren (Schlosssymbol)*, um das alte Persistent Volume zu entsperren. Gebt die Passphrase des alten Volumes ein und klickt auf *Entsperren.*

6. Wählt die Partition *TailsData* aus, die unter der LUKS-Partition erscheint.

7. Klickt auf die Schaltfläche *Einhängen* (►). Das alte Persistent Volume ist nun unter */media/amnesia/TailsData* eingehängt.

Kopieren der alten Dateien in das neue Persistent Volume:

1. Wählt *Anwendungen* ► *Systemwerkzeuge* ► *Root Terminal* aus, um ein Terminal mit Administrationsrechten zu öffnen.

2. Gebt den Befehl `nautilus [Enter]` ein, um den Dateimanager mit Administrationsrechten auszuführen.

3. Navigiert im Dateimanager zu */media/amnesia/TailsData*, um das alte Persistent Volume zu öffnen.

4. Wählt in der Titelleiste *Menü* ► *Neuer Reiter* aus und navigiert in diesem neuen Reiter zu dem Ordner */live/persistence/TailsData_unlocked.*

5. Wählt den *TailsData*-Reiter aus.

6. Um einen Ordner, der persistente Daten enthält, vom alten Persistent Volume in das neue zu kopieren, zieht diesen Ordner aus dem Reiter *TailsData* und lasst ihn über dem Reiter *TailsData_unlocked* los.

Wählt beim Kopieren von Ordnern die Option *Diese Aktion auf alle Dateien* anwenden und klickt auf *Zusammenführen*, um es auf alle Unterordner anzuwenden. Anschließend könnte es notwendig sein, die Option *Aktion auf alle Dateien anwenden* auszuwählen und auf *Ersetzen* zu klicken, um sie auf alle Dateien anzuwenden.

Kopiert am besten nur die Ordner von den Funktionen, die ihr beim Anlegen des alten persistent Volumes aktiviert hattet:

- Der *apt*-Ordner entspricht der APT-Pakete- und APT-Listen-Funktion des beständigen Speicherbereichs. Aber sie benötigt Administrationsrechte, um importiert zu werden und dies sprengt den Rahmen dieser Dokumentation. Dieser Ordner enthält keine persönlichen Daten.
- Der *bookmarks*-Ordner enthält die Lesezeichen des Browsers.
- Der *cups-configuration*-Ordner enthält eure persönlichen Drucker-Einstellungen.
- Der *dotfiles*-Ordner (Punktdateien) beinhaltet versteckte System-Konfigurationsdateien.
- Der *electrum*-Ordner enthält die BitCoin-Einstellungen.

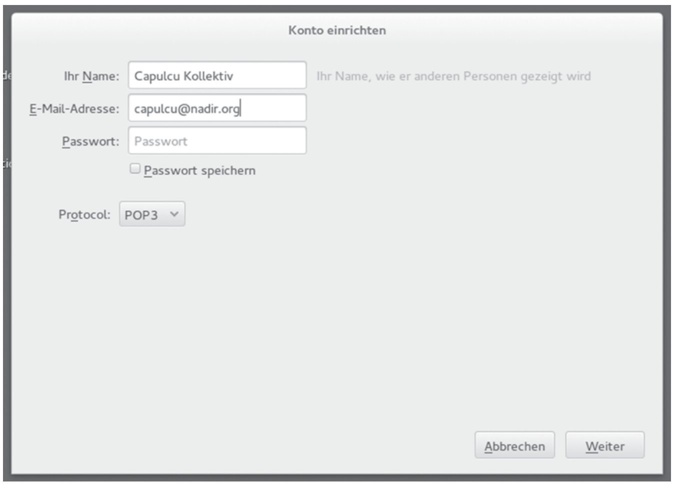
- Der *gnome-keyring*-Ordner und der *gnupg*-Ordner enthalten die pgp-Schlüssel.
- Der *thunderbird*-Ordner enthält die Mail-Einstellungen sämtlicher Mail-Konten, die ihr mit Thunderbird verwaltet.
- Der *nm-connections*-Ordner enthält die gemachten Netzwerk-Einstellungen .
- Der *openssh-client*-Ordner enthält SSH-Schlüssel.
- Der *Persistent-Ordner* entspricht der Persönliche Dateien Funktion des beständigen Speicherbereichs. Den benötigt ihr in jedem Fall!

7. Schließt nach dem Durchführen der Kopie den Dateimanager.

Thunderbird - Mailen mit Persistenz

Tails enthält das Mailprogramm *Mozilla Thunderbird*. Mit Thunderbird und der Persistenz von Tails könnt ihr Mails schreiben, lesen, verschlüsseln, entschlüsseln und eure Mails, Schlüssel und Einstellungen verschlüsselt auf dem Tails Stick speichern. Somit könnt ihr auf diese auch nach einem Neustart zugreifen. Voraussetzung dafür ist, dass ihr beim Erstellen des persistenten Speichers *GnuPG* und *Thunderbird* aktiviert habt.

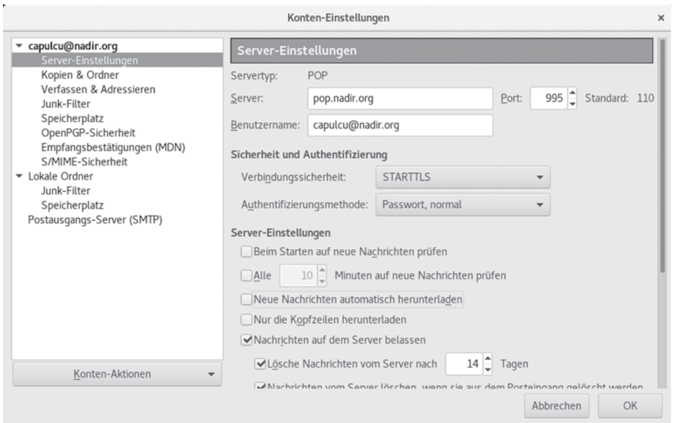
Thunderbird startet ihr entweder über das Icon links in der Toolbar oder unter *Anwendungen* ▸ *Internet* ▸ *Thunderbird*. Beim ersten Start führt euch ein Setup-Assistent durch die Konfiguration eures E-Mail-Postfaches. Es müssen zuerst der Name und die E-Mail-Adresse eingegeben werden. Das Passwortfeld kann freigelassen werden und die *Passwort speichern*-Checkbox sollte nicht mit einem Häkchen markiert sein, da euer Passwort nicht gespeichert werden soll. Mit dieser Einstellung werdet ihr nach jedem Start des Programms nach eurem Passwort gefragt.



Sollen die E-Mails aus dem Postfach auch von anderen Menschen mit anderen Computern abgerufen werden können, muss als Protokoll IMAP ausgewählt werden, ansonsten empfehlen wir das Protokoll POP3, bei dem die E-Mails vom Server heruntergeladen werden und danach nur auf dem verschlüsselten Stick vorhanden sind.

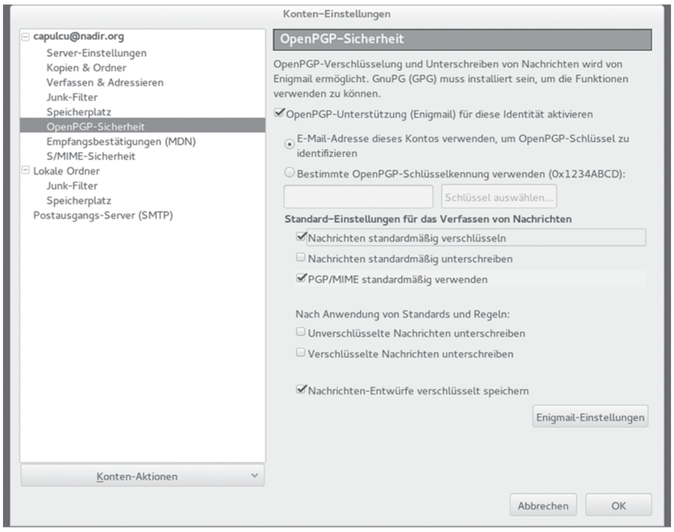
Nachdem ihr auf *Weiter* geklickt habt, erscheint eine Meldung, die euch sagt, dass die weitere automatische Konfiguration deaktiviert wurde, um eure Privatsphäre zu schützen. Dies könnt ihr bestätigen. Nun beginnt die eigentliche Konfiguration:

Wisst ihr die Werte für den Server, Port und Benutzer*innenname für eure E-Mail-Adresse nicht auswendig, könnt ihr entweder in eurem bisherigen Mail-Programm wie Thunderbird oder auf der Internetseite eures Mailanbieters diese Einstellungen nachschauen. Wichtig ist, dass bei *Verbindungssicherheit* entweder der *SSL/TLS* oder *STARTTLS* ausgewählt wird. Die *Authentifizierungsmethode* könnt ihr meist einfach auf *Passwort, normal* belassen. Beide Angaben könnt ihr aber ebenfalls in eurem bisherigen Mail-Programm oder auf der Internetseite eures Mailanbieters nachschauen. Wir empfehlen die fünf Häkchen in der Rubrik *Server-Einstellungen* zu entfernen. In der Rubrik *Nachrichtenspeicher* müsst ihr keine Veränderungen vornehmen, könnt aber auswählen, dass bei jedem Verlassen der Papierkorb geleert wird. Das hat den Vorteil, dass gelöschte Mails mit sensiblen Daten nicht noch weiter gespeichert werden.



Unter den Menüpunkten *Kopien & Ordner, Verfassen & Adressieren, Junk-Filter* und *Speicherplatz* müssen keine Änderungen vorgenommen werden.

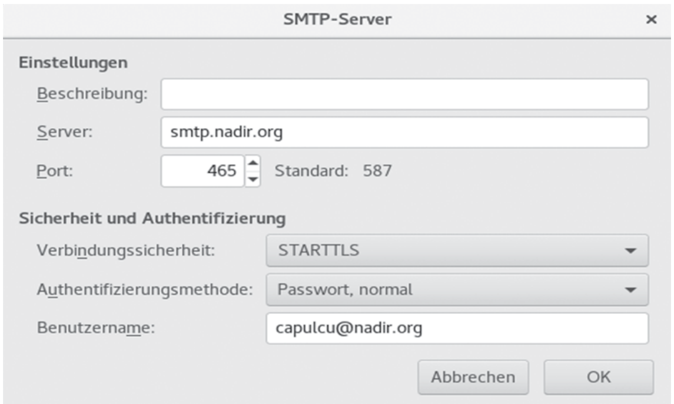
Unter dem Menüpunkt *OpenPGP-Sicherheit* solltet ihr folgende Änderungen vornehmen:



Der oberste Haken bei *OpenPGP-Unterstützung (Enigmail) für diese Identität aktivieren* muss gesetzt werden. Danach sollte *E-Mail-Adresse dieses Kontos verwenden, um OpenPGP-Schlüssel zu identifizieren* ebenfalls ausgewählt werden. Wir empfehlen die drei Einstellungen *Nachrichten standardmäßig verschlüsseln, PGP/MIME standardmäßig verwenden* und *Nachrichten-Entwürfe verschlüsselt speichern* zu aktivieren und die drei restlichen Einstellungen deaktiviert zu lassen.

Unter den Menüpunkten *Empfangsbestätigungen, S/MIME-Sicherheit* und in den Unterpunkten des *Lokalen Ordners* müsst ihr keine Anpassungen vornehmen. Es bleibt die Konfiguration des *Postausgangs-Servers (SMTP)*:

Nachdem ihr den Menüpunkt angeklickt habt, erscheint rechts eine als Standard markierte Konfiguration. Diese bearbeitet ihr mit einem Klick auf *Bearbeiten* und erhaltet folgendes Fenster:

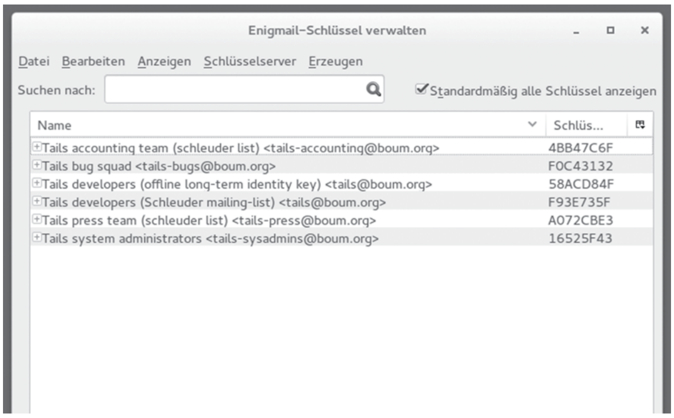


Hierbei kann die Beschreibung leer gelassen werden. Die hier weiter benötigten Einstellungen bekommt ihr alle von der Internetseite eures Mailanbieters oder ihr schaut, welche Einstellungen ihr bisher in eurem E-Mailprogramm stehen habt.

Wichtig ist hierbei wieder, dass bei dem Punkt *Verbindungssicherheit* entweder *SSL/TLS* oder *STARTTLS* ausgewählt ist. Der Name des SMTP-Servers beginnt oft mit *smtp* und der zugehörige Port lautet oft 465. Die *Authentifizierungsmethode* kann meist unverändert übernommen werden. Der *Benutzername* ist meist entweder die gesamte Mail-Adresse oder der Teil vor dem @.

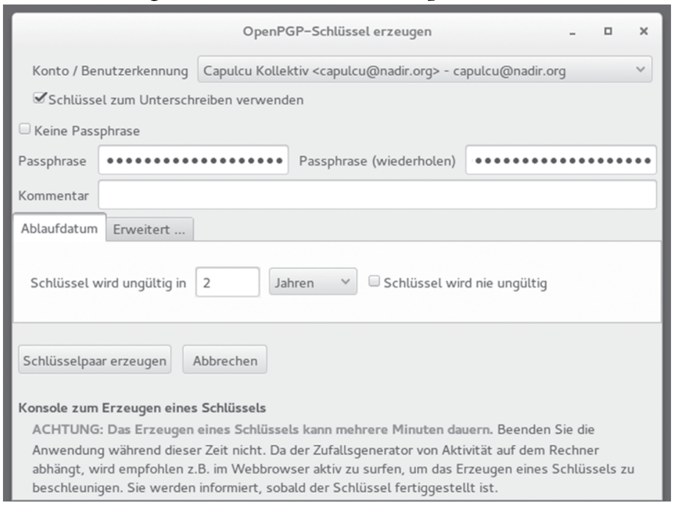
Nun ist die E-Mail-Adresse fertig konfiguriert und sowohl das Fenster der SMTP-Server-Konfiguration als auch die Konteneinstellungen können mit „*OK*“ bestätigt werden.

Nun fehlt nur noch die Einrichtung der GPG/PGP-Verschlüsselung. Die Schlüsselverwaltung wird in Thunderbird mit dem Plugin *Enigmail* durchgeführt. Um neue Schlüssel hinzuzufügen geht ihr rechts im Anwendungsmenü von Thunderbird auf *Enigmail* ► *Schlüssel verwalten …*



Habt ihr bereits ein Schlüsselpaar, das ihr weiterverwenden wollt, oder möchtet ihr öffentliche Schlüssel von Freund*innen hinzufügen, dann habt ihr zwei Möglichkeiten. Entweder ihr kopiert die Schlüssel in einem anderen Programm wie zum Beispiel einem Texteditor in die Zwischenablage, dann könnt ihr sie mit *Bearbeiten* ► *Aus Zwischenablage einfügen* hinzufügen. Die zweite Möglichkeit ist, die Schlüsseldatei mit *Datei* ► *Importieren* hinzuzufügen. Dabei müsst ihr unter Umständen in dem *Datei Öffnen Dialog* rechts unten *Alle Dateien* zum Anzeigen auswählen, da sonst nur Dateien mit der Endung *gpg* angezeigt werden.

Habt ihr noch kein eigenes Schlüsselpaar, könnt ihr dieses unter *Erzeugen* ► *Neues Schlüsselpaar* nun erstellen:

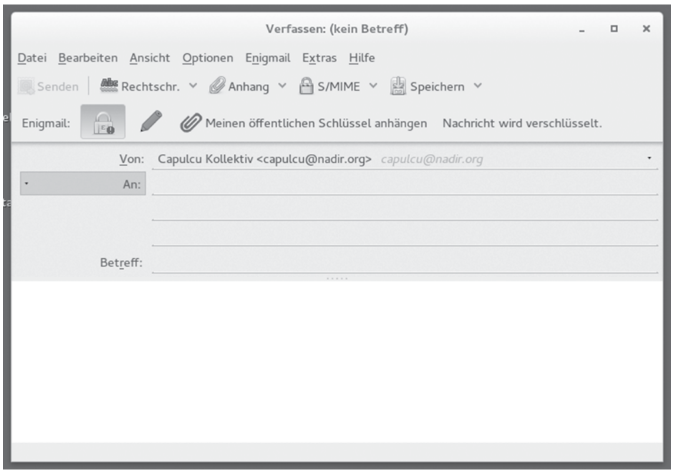


Hier sollte das Häkchen bei *Schlüssel zum Unterschreiben verwenden* gesetzt sein und die Passphrase nach den Regeln des Kapitels zu Passwortsicherheit gewählt werden. Der Kommentar muss nicht ausgefüllt werden. Das Ablaufdatum sollte nicht zu lang gewählt werden, also je nach Verwendung der E-Mail-Adresse nicht über 4 Jahre, denn sollte jemals der private Schlüssel und die Passphrase in falsche Hände gelangen, können alle Mails aus dieser Zeit entschlüsselt werden.

Die Häkchen bei *Keine Passphrase* und *Schlüssel wird nie ungültig* sollen niemals gesetzt werden! Unter dem Reiter *Erweitert …* ist darauf zu achten, dass die Schlüsselstärke 4096 beträgt. Sind alle Einstellungen gesetzt, kann das Schlüsselpaar erzeugt werden. Dies muss noch einmal mit *Schlüssel erzeugen* bestätigt werden. Die Erzeugung kann einige Zeit in Anspruch nehmen. Es folgt eine Frage, ob ein Widerrufszertifikat erstellt werden soll. Dieses könnt ihr erstellen und auf dem Stick verschlüsselt speichern. Ihr benötigt es nur, wenn euer privater Schlüssel in fremde Hände gelangt ist.

Nun seht ihr in der Schlüsselübersicht neben den Schlüsseln von Tails die von euch hinzugefügten oder erstellten Schlüssel. Einzelne Schlüssel könnt ihr mit der *rechten Maustaste ► In Datei Exportieren* in einer Datei speichern. Achtet darauf, dass ihr nur den öffentlichen (nicht den privaten) Schlüssel exportiert, wenn ihr diesen weitergeben wollt.

Wenn ihr das *Enigmail Schlüssel verwalten* - Fenster nun schließt, könnt ihr mit einem Klick auf *Verfassen* eine neue E-Mail verfassen.



Wichtig ist beim Verfassen einer E-Mail, dass der Button neben dem Wort Enigmail ein geschlossenes Schloss zeigt und der Text *Nachricht wird verschlüsselt* am Ende dieser Zeile angezeigt wird, wie auch oben zu sehen ist. Wollt ihr die Nachricht zusätzlich signieren, könnt ihr das mit einem Klick auf den Stift machen. Wollt ihr euren öffentlichen Schlüssel an die Mail hängen, so dass die Empfänger*in euch auch wieder verschlüsselt zurückschreiben kann, klick die Büroklammer an. Wollt ihre andere öffentliche Schlüssel anhängen, könnt ihr diese in dem Menü *Enigmail ► Öffentliche Schlüssel anhängen* auswählen. Sendet ihr die Mail und habt Signieren ausgewählt, müsst ihr zuerst eure GPG/PGP Passphrase eingeben und darauf dann euer E-Mail-Passwort. Schickt ihr die Mail, ohne sie zu signieren, müsst ihr nur euer E-Mail-Passwort eingeben.

Beim Abrufen der Mails müsst ihr zuerst auch euer E-Mail-Passwort eingeben und falls ihr verschlüsselte Mails bekommen habt, werdet ihr noch der GPG/PGP-Passphrase gefragt. Beim Betrachten von eingegangenen Mails symbolisiert ein geschlossenes Schloss am oberen Rand der Nachricht, dass die Nachricht verschlüsselt ist und ein Briefumschlag, dass diese signiert ist.

Anhang

Hier stellen wir euch vor, wie ihr die jeweils aktuelle Version von Tails *herunterladen und überprüfen(!)* könnt, um daraus eine(n) „bootfähige" Tails-DVD oder einen USB-Stick zu erstellen.

Da einige Menschen abhängig vom Rechner und dessen BIOS-Einstellmöglichkeiten *Schwierigkeiten beim Booten* von einem der Startmedien haben, gehen wir kurz auf die häufigsten Fallstricke ein.

Falls euch (wider Erwarten) dennoch das erstmalige Starten von Tails nicht gelingen sollte, holt euch *einmalig* Hilfe bei der BIOS-Einstellung, oder bei der Überprüfung der Tails-Version auf ihre Echtheit - das ist kein hinreichender Grund, auf die *viel einfachere Benutzung* von Tails zu verzichten!

Abschließend geben wir euch Tipps zur Wahl und Handhabung von möglichst sicheren Passwörtern.

Wie bekomme ich Tails

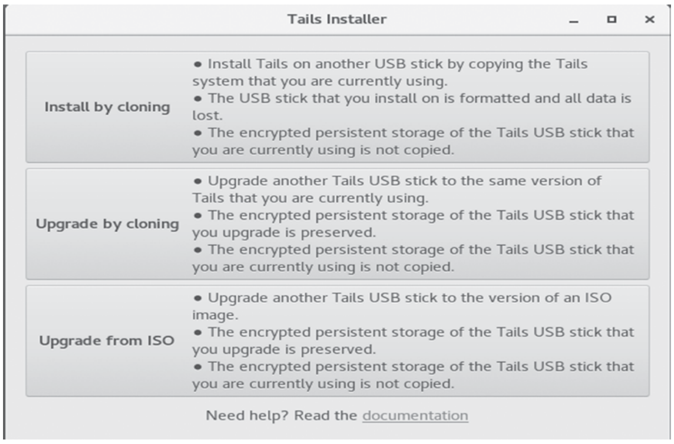
Im Kapitel „*Warnung: Grenzen von Tails*" haben wir die Praxis von *Man-in-the-Middle*-Angriffen diskutiert, bei denen sich die Angreifer*in in die Datenströme hängt, um sie zu *kontrollieren* und/oder zu *manipulieren*. Insbesondere beim Herunterladen von Software ist daher darauf zu achten, deren „Echtheit" zu überprüfen. Andernfalls kann euch leicht ein manipuliertes Tails untergeschoben werden.

Wer auf eine bereits überprüfte Version von Tails zurückgreifen kann, hat es mit dem nun folgenden Kapitel *Tails Installer* zum Erzeugen eines neuen / weiteren Tails-Stick leicht. Im Kapitel *Tails Upgrader* lernt ihr, wie ihr Euer Tails automatisch aktuell haltet.

Danach lernen alle anderen, die Überprüfung und Erstellung eines Tails-Startmediums eigenständig zu erledigen. Dieser Teil der Anleitung mag euch kompliziert erscheinen - aber ihr dürft ihn nur dann ignorieren, wenn euch eine Person eures Vertrauens mit einer „geprüften" Tails-Version versorgt hat.

Tails-Installer

Wenn ihr schon ein lauffähiges Tails-System auf einem USB-Stick oder einer DVD habt und einen weiteren USB-Stick (keine DVD) erstellen wollt, könnt ihr den „*Tails Installer*" verwenden. Den „*Tails Installer*" findet ihr unter *Anwendungen* ► *Tails* ► *Tails Installer*. Wenn ihr ihn startet, erhaltet ihr den folgenden Bildschirm, auf dem ihr zwischen drei Möglichkeiten auswählen könnt:



„*Klonen & Installieren*" wählt ihr aus, wenn ihr die Tails Version des laufenden System auf einen anderen USB-Stick übertragen wollt. Alle Daten auf dem anderen USB-Stick werden dabei gelöscht. Es wird ausschließlich das Tails System übertragen, nicht eventuell vorhandene Daten der Tails-Persistenz.

„*Klonen & Aktualisieren*" wählt ihr aus, wenn auf dem zu beschreibenden USB-Stick bereits ein Tails-System vorhanden ist und ihr dieses nur mit dem aktuelleren Tails, von dem ihr gerade gestartet habt, überschreiben möchtet. Eventuell vorhandene Daten der Tails-Persistenz werden auf dem Datenträger nicht überschrieben. Auch hier werden keine Daten der Tails-Persistenz des aktuell gestarteten Systems übertragen.

„*Von ISO aktualisieren*" wählt ihr aus, wenn auf dem zu beschreibenden USB-Stick bereits ein Tails-System vorhanden ist und ihr dieses mit einem heruntergeladenen ISO-Abbild einer neueren Tails Version überschreiben möchtet.



Spätestens nachdem ihr euch für eine Funktion entschieden habt, müsst ihr den USB-Stick einstecken, der das neue Tails-System erhalten soll. Um zu vermeiden, den falschen USB-Stick zu löschen, solltet ihr darauf achten, dass außer dem originalen und dem zukünftigen Tails-Stick keine anderen USB-Sticks oder SD-Karten eingesteckt sind. Ist dies der Fall, wird im nächsten Fenster als „*Zielmedium*" nur eine Option - euer eingesteckter USB-Stick - vorhanden sein (siehe Abbildung). Andernfalls muss der gewünschte USB-Stick als Zielmedium ausgewählt werden. Nachdem ihr nun auf „*Tails installieren*"

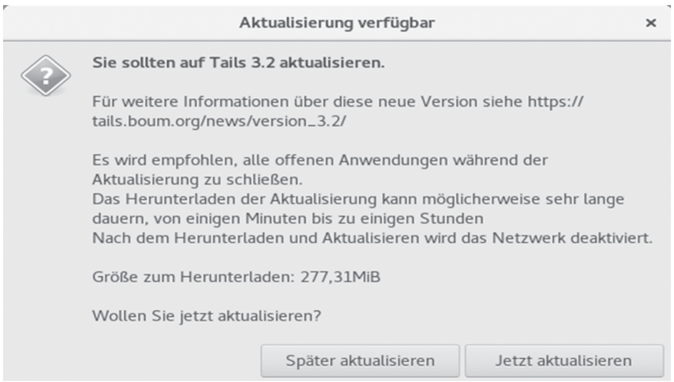
geklickt habt, müsst ihr noch einmal bestätigen, dass ihr auch wirklich diesen Stick überschreiben möchtet. Danach kann die Erstellung des neuen Sticks ein paar Minuten in Anspruch nehmen. Ausschließlich bei der dritten Option *„Von ISO aktualisieren“* müsst ihr zusätzlich noch das zu verwendende, bereits heruntergeladene Live-System-ISO-Abbild auswählen.

Tails-Upgrader

Bei jedem Start von Tails wird direkt nachdem die Verbindung zu dem Tor-Netzwerk hergestellt wurde überprüft, ob die aktuelle Tails Version verwendet wird.

Es ist wichtig, immer die aktuelle Version zu verwenden, da regelmäßig Sicherheitslücken in den von Tails verwendeten Programmen entdeckt werden, die im schlimmsten Fall dazu führen, dass eure Identität, eure IP-Adresse, etc. nicht verschleiert werden. Durch ein Tails Upgrade werden diese Sicherheitslücken gestopft und meist auch andere Fehler behoben.

Falls ihr Tails mit DVD verwendet oder Tails manuell auf den USB-Stick gespielt habt ohne die Verwendung des Tails Installers, bekommt ihr die Meldung „You should do a manual Upgrade“. Das heißt, ihr solltet manuell eine neue Version von Tails herunterladen, überprüfen und auf DVD brennen oder auf einen USB-Stick spielen.



Habt ihr jedoch euer Tails mit dem Tails Installer auf einen USB-Stick gespielt, habt ihr nun Glück, denn in diesem Fall macht der Tails Upgrader für euch die Arbeit. Ihr werdet gefragt ob ihr ein Upgrade sofort oder später durchführen wollt. Wenn ihr auf „Upgrade Now“ klickt, wird das Upgrade automatisch heruntergeladen und überprüft. Dies erspart euch die aufwendigere Überprüfung der Checksumme, die ihr durchführen solltet, wenn ihr ein ISO-Abbild herunterladet. Wenn der Download-Vorgang beendet ist, wird das Upgrade auf eurem USB-Stick installiert. Nach einem Neustart ist das Tails-System auf dem aktuellen Stand. Daten auf einer eventuell vorhandenen Tails-Persistenz sind davon nicht betroffen und bleiben weiterhin bestehen. Falls ein Stick mit Schreibschutzschalter verwendet wird, müsst ihr diesen natürlich für die eine Sitzung, in der ihr das Upgrade durchführt, auf „beschreibbar“ stellen.



Bekommt ihr allerdings nach dem Start von Tor die Meldung „Nicht genügend Speicher vorhanden, um nach Aktualisierungen zu suchen“, hat euer Rechner zu wenig Arbeitsspeicher oder ihr habt schon speicherhungrige Programme wie LibreOffice oder den Tor-Browser gestartet. In diesem Fall kann es helfen, nach einem Neustart und der Meldung „*Tor* ist bereit“ zunächst keine weiteren Programme zu starten.

Digitale Signaturen

Durch digitale Signaturen kann die „Echtheit“ einer Software überprüft werden. Hierfür wird der öffentliche PGP-Schlüssel des Entwickler*innen-Teams benötigt, mit dem die Software unterschrieben wurde. Die Unterschrift garantiert, dass es sich um eine unveränderte Version der bezogenen Software handelt.

Wenn ihr euch z.B. die aktuelle Version der Live-DVD Tails besorgt, findet ihr im Download-Bereich eine entsprechende Signatur, mit der ihr die „Echtheit“ der Software überprüfen könnt. Dafür benötigt ihr noch den PGP-Schlüssel der Entwickler*innen, der ebenfalls auf der Download-Seite erhältlich ist. Nach erfolgreichem Import dieses Schlüssels könnt ihr über grafische Tools oder über eine sogenannte Kommandozeile die Authentizität der Software überprüfen. Wie dies funktioniert stellen wir euch in den nächsten Kapiteln vor.

Theoretisch wäre es durch einen Man-in-the-Middle-Angriff trotzdem noch möglich, euch eine falsche Signatur und eine dafür angepasste Software, sowie einen falschen Schlüssel zu übermitteln. Ein Weg dies zu umgehen, ist, die Software und deren Signatur über verschiedene Netzwerke zu besorgen - z.B. einmal von eurer Arbeit aus, dann von eurem Anschluss zu Hause und ein zusätzliches mal über *Tor*.

Tails herunterladen und überprüfen

Die Echtheit eurer heruntergeladenen Tails-Version solltet ihr über die PGP-Signatur der Tails-Entwickler*innen überprüfen. Wir beschreiben im Folgenden das Vorgehen für Linux- und Mac-Nutzer*innen.

Tails liegt auf dem Server *https://tails.boum.org* zum Download bereit. Leider ist es möglich, dass ein Angreifer die Daten auf dem Weg zu euch abfängt und modifiziert. Wir beschreiben im Folgenden, wie ihr eine solche Modifikation sicher identifizieren könnt und deshalb auch sicher sein könnt, dass die Daten, die ihr runtergeladen habt, auch die richtigen sind. Wir beschreiben das hier für Linux und MacOS X User*innen - Windows User*innen müssen wir auf die Anleitung auf https://tails.boum.org verweisen.

Ihr braucht drei Dateien, die ihr vom Tails-Server runterladen müsst:

- Das Image der Tailssoftware selbst
- Die Signatur, welche die Echtheit bestätigt
- Den public-key der Tails-Entwickler*innen, mit dem die Signatur gemacht wurde

Ihr könnt das mit dem Webbrowser machen oder von der Kommandozeile aus - zuerst laden wir den public-key und binden ihn ein:

Für Eingaben per Kommandozeile müsst ihr zunächst ein *Terminal* öffnen. Die Kommandozeilen in diesem Heft sind alle ohne Silbentrennung gedruckt; d.h. ihr müsst alle Minus-Zeichen auch am Zeilenende eintippen. Ihr findet diese Anleitung auch auf unserer Webseite *https://capulcu.blackblogs.org*, so dass ihr die Kommandos auch dort mit der Maus in die Zwischenablage kopieren und im *terminal* einfügen könnt. Die Kommandozeilen-Eingabe wird jeweils mit der Eingabetaste [ENTER] abgeschlossen.

Linux

1) Tails-Schlüssel herunterladen und importieren:

```
wget https://tails.boum.org/tails-signing.key
[ENTER]
```

```
gpg --import tails-signing.key
[ENTER]
```

Die Ausgabe sollte wie folgt aussehen:

```
gpg: key DBB802B258ACD84F: public key „Tails
developers (offline long-term identity key)
<tails@boum.org>" imported

gpg: Total number processed: 1

gpg:               imported: 1  (RSA: 1)
```

(wenn du den Schlüssel das erste Mal importierst)

oder

```
gpg: key DBB802B258ACD84F: „Tails developers
(offline long-term identity key) <tails@boum.
org>" not changed

gpg: Total number processed: 1

gpg:              unchanged: 1
```

(wenn der Schlüssel bereits importiert war)

Wir überprüfen nun, ob der importierte Key echt, d.h. unverändert ist:

```
gpg --fingerprint 0xDBB802B258ACD84F | grep
fingerprint [ENTER]
```

```
Key fingerprint = A490 D0F4 D311 A415 3E2B  B7CA
DBB8 02B2 58AC D84F:
```

Die Ausgabe bei euch muss identisch sein, andernfalls ist das schief gegangen.

In diesem Fall löscht den falschen Key mit `gpg --delete-key DBB802B258ACD84F` und versuche diese Prozedur von einem anderen Internet-Anschluss aus nochmal. Auf keinen Fall mit dem falschen Key weitermachen!

2) Tails herunterladen: (>1GB - das dauert eine Weile)

Dazu mit dem Webbrowser auf die Seite

https://tails.boum.org/install/download/openpgp/index.en.html

gehen und die Software hinter dem Link „*Download the Tails 3.1 ISO image (1.2 GiB).*" runterladen. Beim Schreiben dieses Textes ist 3.1 die aktuelle Version, das wird sich natürlich im Laufe der Zeit ändern.

3) Tails-Signatur herunterladen:

Auf der gleichen Seite findet ihr den Link „*Download the Tails 3.1 OpenPGP signature*", ladet diese (aktuell: tails-amd64-3.1.iso.sig) runter.

4) Tails mit der Signatur überprüfen:

Jetzt zum magischen Schritt: die Überprüfung der Signatur und damit die Sicherstellung, ob die Tails-Software modifiziert wurde oder nicht.

```
gpg --verify tails-amd64-3.1.iso.sig tails-
amd64-3.1.iso [ENTER]
```

Die Ausgabe sollte nach zusätzlichen gpg-Statusmeldungen wie folgt aussehen:

```
gpg: Signature made Mon 25 Apr 2016 07:02:56
PM CEST
gpg:                using RSA key 0x98FEC6B-
C752A3DB6
```

```
gpg: Good signature from „Tails developers
(offline long-term identity key) <tails@boum.
org>“
gpg:                 aka „Tails developers
<tails@boum.org>“
gpg: WARNING: This key is not certified with a
trusted signature!
gpg:          There is no indication that the
signature belongs to the owner.

Primary key fingerprint: A490 D0F4 D311 A415
3E2B  B7CA DBB8 02B2 58AC D84F

     Subkey fingerprint: BA2C 222F 44AC 00ED
9899  3893 98FE C6BC 752A 3DB6
```

ACHTUNG: Überprüfe, ob *„Good signature ...“* erscheint. Wenn dem so ist, und nur dann(!), fahre fort. Andernfalls, entferne die heruntergeladenen Dateien (mit dem Kommando `rm tails-amd64-3.1.iso [ENTER]`), wechsele den Ort bzw. die Internetverbindung und lade Tails erneut herunter

```
exit [ENTER] (Terminal wird geschlossen)
```

Mac

Während bei allen Linux-Distributionen das Programm *gpg* bereits installiert ist, müssen MAC OS X-Nutzer*innen einmalig das Programm **gpgtools** von *https://gpgtools.org* herunterladen.

Desweiteren verwenden MAC-Nutzer*innen das Kommando `curl -O` statt `wget` und zwar mit einem großen „O“ - keine Null! Ansonsten sind alle vier Schritte des vorherigen Abschnitts identisch.

Tails auf USB-Stick installieren

Wir empfehlen zur komfortablen Einrichtung eines Tails-USB-Sticks das Programm „*tails-installer*“ zu benutzen, der seit den Linux-Distributionen *Debian 8* und *Ubuntu 15.10* zur Verfügung steht.

Du benötigst einen USB-Stick mit mindestens 4 GB Speicherplatz. ACHTUNG: Alle eventuell vorhandenen Daten auf diesem Stick werden gelöscht![55] Wir öffnen wieder ein *Terminal*, um die folgenden Kommandozeilen eintippen oder hinein kopieren zu können.

Debian-Linux

```
su - [ENTER]

[PASSWORT EINGEBEN][ENTER]

echo „deb http://ftp.debian.org/debian
stretch-backports main“ > /etc/apt/sources.
list.d/stretch-backports.list [ENTER]

apt-get update [ENTER]

apt-get -y install tails-installer [ENTER]

exit [ENTER] (das Terminal wird geschlossen)
```

55 Ein Forensiker könnte die ehemaligen Daten problemlos wiederherstellen. Daher nutze keinen Stick, auf dem zuvor unverschlüsselte, sensible Daten gespeichert waren.

Ubuntu-Linux

```
sudo add-apt-repository ppa:tails-team/tails-
installer [ENTER]

[PASSWORT EINGEBEN] [ENTER]

sudo apt-get update [ENTER]

sudo apt-get -y install tails-installer
syslinux-common [ENTER]

exit [ENTER] (das Terminal wird geschlossen)
```

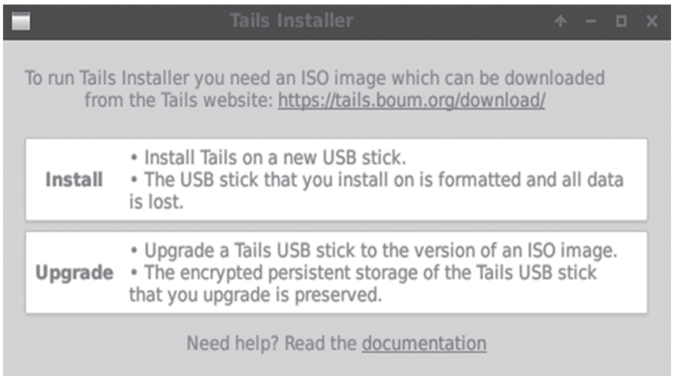
Weiter geht es für alle Linux-Varianten mit der Erstellung des Tails-USB-Sticks.

- Entferne alle möglicherweise an den Computer angeschlossenen USB-Sticks, die du nicht als Tails-Stick verwenden möchtest

- Schließe den USB-Stick an den Computer an, der zukünftig Tails-Stick werden soll. Erinnerung: Alle Daten werden auf diesem Stick gelöscht!

- Starte das Programm „Tails-Installer“ 

- Klicke auf „Install“



- Klicke auf den Button unter „Use existing Live System ISO). Ein Dateibrowser öffnet sich, navigiere in das /home Verzeichnis deines Benutzers und klicke doppelt auf „tails-amd64-3.1.iso“ oder eine entsprechend neuere Version (NICHT „tails-amd64-3.1.iso.sig“).

- In dem Feld unter „Target Device“ sollte nun *„tails-amd64-3.1.iso selected“* stehen.

- Klicke ganz unten auf „Install Tails“. Das dann erscheinende Fenster fragt dich um Bestätigung, weil alle Daten auf dem USB-Stick gelöscht werden

- Wenn du dir sicher bist, klicke „Yes“

- Andernfalls klicke „No“, und wechsele den USB-Stick

- Der nachfolgende Prozess dauert eine Weile. Auf keinen Fall den Stick ziehen! Danach könnt ihr den Tails-Installer schließen.

Mac

Da es für Mac OS X derzeit keinen *Tails-installer* gibt, müsst ihre das heruntergeladene und überprüfte Tails (aktuell: *tails-amd64-3.1.iso*) in einem Zwischenschritt auf DVD brennen. Wie das geht, ist im nächsten Kapitel erklärt. Mit der so gebrannten DVD könnt ihr nach dem ersten Tails-Start den dort vorhandenen Tails-installer benutzen, um einen Tails-USB-Stick zu erzeugen. Erinnerung: Zum Starten von Tails müsst ihr beim Booten die Alt-Taste gedrückt halten und Tails anschließend als Startvolume auswählen.

Tails auf DVD brennen

Wer keinen USB-Stick für das Tails-Betriebssystem benutzen möchte oder kann, muss sich mit einer DVD behelfen. Vorteil: Die einmal gebrannte DVD ist automatisch gegen nachträgliche Veränderung „schreibgeschützt". Nachteil: Ihr müsst für jede aktuelle Tails-Version (etwa alle 2 Monate) eine neue DVD brennen.

Nachdem ihr nun davon ausgehen könnt, dass ihr eine korrekte Version von Tails besitzt (z.B. *tails-amd64-3.1.iso),* muss das Betriebssystem auf eine DVD gebrannt werden. Verwendet dafür am besten eine *nicht-wieder-beschreibbare DVD* mit der Bezeichnung: DVD + R. Sie sollte auf keinen Fall die Bezeichnung DVD + RW oder DVD + RAM besitzen.

Linux

Tails könnt ihr euch unter Ubuntu oder Debian auf DVD brennen, indem ihr mit der *rechten Maustaste* aus die überprüfte Tails.iso Datei (z.B. *tails-amd64-3.1.iso*) klickt und *„Open With Brasero Disc Burner" („Mit Brasero öffnen")* auswählt. Mit einem Bestätigen über den Button *„Create Image" („Abbild erstellen")* wird Tails auf eine DVD gebrannt.[56]

Mac

Um Tails auf eine DVD zu brennen, müsst ihr das *„Festplattendienstprogramm"* unter *„Programme/Dienstprogramme"* öffnen und die Tails.iso Datei (z.B. *tails-amd64-3.1.iso)* dort hinein ziehen. Danach kann das Live-System über den Button *„Brennen"* auf eine DVD gebrannt werden.

Alternativ könnt ihr Tails auch über das *„Festplattendienstprogramm"* durch „► *Images* ► *Brennen*" dauerhaft auf eine DVD bringen.

56 Für neuere Ubuntu-Versionen (nach 12.10) findet ihr eine Anleitung zum Erstellen der DVD unter folgender Webseite: https://help.ubuntu.com/community/BurningIsoHowto



Bootreihenfolge im BIOS ändern

Um euren Rechner in die Lage zu versetzen, ein Betriebssystem von DVD bzw. vom USB-Stick starten (=„booten") zu können, müsst ihr in der Regel die „Boot-Reihenfolge" im sogenannten BIOS ändern. Das BIOS ist sozusagen das Basis-Betriebssystem eines Rechners, das grundlegenden Rechnerfunktionen an/ausschaltet und festlegt, in welcher Reihenfolge beim Start auf welchen Datenträgern nach bootfähigen Betriebssystemen gesucht werden soll.

- Datenträger einlegen/einstecken und Computer neu starten.
- Unmittelbar nach dem Start eine der Tasten F1, F2, DEL, ESC, F10 oder F12 gedrückt halten (auf einen Hinweis auf dem kurz erscheinenden Startbildschirm achten), um in das BIOS-Setup zu gelangen. Die meisten Rechner bieten nur ein englisch-sprachiges BIOS-Menü. Wir listen im Folgenden (abhängig vom Computerhersteller) die *wahrscheinlichsten* Tasten, um zu den BIOS-Einstellungen zu gelangen[57]:

Acer	Esc, F12, F9
Asus	Esc, F8
Dell	F12
Fujitsu	F12, Esc
HP	Esc, F9
Lenovo	F12, Novo, F8, F10
Samsung	Esc, F12, F2
Sony	F11, Esc, F10
Toshiba	F12
andere	F12, Esc

- Suche im Menü nach *„Edit Boot Order"* (Boot-Reihenfolge ändern).
- Setze den Eintrag *„DVD"* oder aber einen der Einträge *„removable drive"*, *„external USB disk"* oder *„USB media"* an den Anfang der Liste der zu durchsuchenden Geräte. Auf jeden Fall vor den Listeneintrag eurer internen Festplatte *„HD"* oder *„harddisk"*.
- Danach mit *„Save changes and exit"* das BIOS verlassen und den Betriebsystemstart fortsetzen. Jetzt sollte der Rechner die geänderte Boot-Reihenfolge berücksichtigen.

57 https://craftedflash.com/info/how-boot-computer-from-usb-flash-drive

Booten „fremder Systeme" zulassen

Falls Tails trotz geänderter Boot-Reihenfolge nicht startet, und der Tails-Stick bzw. die Tails-DVD korrekt erstellt wurde[58], dann überprüft bei neuerem Computer, ob ihr im BIOS eine der folgenden Funktionen finden und auswählen könnt:

- Enable Legacy mode
- Disable Secure boot
- Enable CSM boot
- Disable UEFI
- Disable Fastboot

Wenn Tails nicht vom USB-Stick startet

- Bootreihenfolge im BIOS überprüfen – sucht das BIOS wirklich auf einem externen USB-Gerät bevor die Festplatte durchsucht wird?
- Ältere Rechner (vor 2001) sind teilweise nicht in der Lage von USB zu „booten".
- Andere externe USB-Geräte zum Start abziehen.
- Verwende einen anderen USB-Anschluss – Das BIOS mancher Rechner überprüft bei der Suche nach bootfähige Datenträgern nicht alle der vorhandenen USB-Anschlüsse.
- Überprüfe, ob der Stick wirklich „bootfähig" ist. Führe erneut die Schritte zum „Brennen" des USB-Sticks durch. Es genügt nicht, die Dateien auf den Stick zu „kopieren".

Mac booten

Beim Hochfahren eures Macs müsst ihr die *Alt-Taste* oder die *C-Taste* gedrückt halten, damit anschließend die Tails-DVD als Startmedium bestimmt wird (oft wird sie fälschlicherweise als Windows-CD angezeigt). Alternativ könnt ihr sie auch unter *„Systemeinstellungen ▸ Startvolume"* auswählen. Bei Mac-Laptops ist das Track-Pad unter Tails oft nicht richtig nutzbar. In diesem Fall hilft eine externe USB-Maus.

58 Einfach durch Test an einem anderen Computer zu überprüfen!

Sicherere Passwortwahl

Es ist immer noch so, dass harte Verschlüsselungstechniken (bei ausreichender Schlüssellänge) „*nicht knackbar*" sind, bzw. der Rechenaufwand für Geheimdienste dazu gigantisch hoch ist.

Hauptangriffspunkt, um an verschlüsselte Daten zu kommen, ist daher meist das verwendete Passwort, mit dem z.B. ein Schlüssel gesichert ist. Mit bereits im Einzelhandel erhältlichen Computern, die leistungsfähige Grafikchips für einfache Rechenoperationen nutzen, ist das Knacken von Passwörtern für Angreifer*innen immer einfacher geworden. Eine Mischung aus simpler Rechenleistung, riesigen Tabellen bereits geknackter Passwörter und clever programmierter Software macht das Passwort-Knacken erschreckend effizient. Daher kommt der richtigen Passwortwahl eine wichtige Bedeutung zu.

ERSTENS: Je „unmenschlicher" desto besser

Rein mathematisch sieht die Lage für uns Passwort-Nutzer*innen gar nicht schlecht aus. Die Zahl aller möglichen Passwörter wächst exponentiell mit deren Länge und der Größe des verwendeten Zeichenraums. Diese muss eine Angreifer*in im Prinzip durchprobieren *(Brute Force-Methode)*, oder aber die Verschlüsselung zur Ablage der Schlüssel auf dem Computer knacken.

> ***Fast alle Angriffe basieren mittlerweile auf Wörterbüchern und Namenslisten erweitert um riesige, gehackte Datenbanken mit mehreren 100 Millionen Passwörtern.***

Die Programme zum Knacken von Passwörtern nutzen darüber hinaus zusätzliche „*Regeln*" *zur Modifizierung* solcher Wörter und orientieren sich dabei an „*menschlichen*" *Mustern* der Veränderung. Die Kombination von Wörtern sowie das Anhängen von Ziffern und insbesondere die *Ersetzung einzelner Buchstaben*, wie das übliche „*3*" statt „*E*" oder „*1*" statt „*i*" oder „*l*" stellen für diese Programme kein Problem dar. Darüber werden selbst sicher aussehende Passwörter wie „*polU09*&l1nk3d1n*" geknackt.

ZWEITENS: Kein Wort für viele Zwecke

Neben der Komplexität des verwendeten Passworts entscheidet die Art, wie es auf eurem Rechner, beim Mail-Anbieter oder Online-Shops abgelegt ist, über dessen Sicherheit.

Kein System sollte Nutzer*innen-Passwörter im Klartext speichern. Aber die Verschlüsselungsmethoden für die Ablage von Passwörtern sind unterschiedlich gut. Beim

eigenen Rechner haben wir bedingt Einfluss darauf, wie leicht unsere Passwörter zu rekonstruieren sind. Bei irgendwelchen Diensten im Internet müssen wir (häufig zu Unrecht) darauf vertrauen, dass damit sorgsam umgegangen wird. Millionen geklauter Kundendaten inklusive Passwörter von unterschiedlichen Service-Anbietern sind eindeutiger und dringender Appell, das dort verwendete Passwort nicht identisch für andere, sensiblere Zwecke zu nutzen!

Vollständig zufällige Passwörter mit mehr als 16 Zeichen gelten auf absehbare Zeit als sicher. Sogar bei Verwendung von Supercomputern – aber sie sind auch sehr schwer zu merken. Daher verwenden viele vermeintlich individuelle Kombinationen, Abkürzungen und Veränderungen existierender Worte. Das macht Passwörter angreifbar.

Nun habt ihr wahrscheinlich Probleme, möglichst lange und komplexe Passwörter für jeden genutzten Dienst erzeugt zu haben, aber merken könnt ihr euch davon bestenfalls drei oder vier. Die einen nutzen daher spezielle Programme wie *KeePassX* (in Tails), die Passwörter in einer sicheren Datei abspeichern und müssen sich daher nur ein *Master-Passwort* merken. Andere nutzen lieber mehrere Basis-Passwörter, aus denen sie dann verschiedene Varianten generieren. Welche Methode ist sicherer? An der Frage scheiden sich die Geister. Wir wollen euch beide Möglichkeiten vorstellen, entscheiden müsst ihr.

Methode I: Verschlüsselte Passwort-Datei

Alle verwendeten Passwörter werden in einer zentralen, *verschlüsselten Datei* gespeichert. Dies hat den Vorteil, sich nur ein Passwort merken zu müssen. So können für alle anderen genutzten Dienste oder Programme auch möglichst sichere und unabhängig voneinander generierte Passwörter genutzt werden. Aber diese Variante hat auch klare Nachteile. Zum einen seid ihr von der einen Datei oder dem einen Programm abhängig. Geht diese verloren oder ihr vergesst das Passwort, verliert ihr damit im Zweifel auch den Zugriff auf alle damit gesicherten Dienste. Das andere große Problem bei dieser Variante ist, wenn jemand an dieses eine **Master-Passwort** herankommt, z.B. über einen eingeschleusten *Keylogger*[59], hat die Person gleichzeitig **Zugriff auf alle anderen Passwörter!**

Um *KeePassX* zu starten, wählt ihr: *Anwendungen* ► *Zubehör* ► *KeePassX*.

Um eine neue Passwortdatenbank zu erstellen, wählt ihr *Datenbank* ► *Neue Datenbank*. Die Passwortdatenbank ist verschlüsselt und durch eine Passphrase geschützt. Dazu gebt ihr eine Passphrase eurer Wahl in das Textfeld *Passwort* ein *(mindestens 16 Zeichen!*) und klickt anschließend auf *OK*. Wiederholt die gleiche Passphrase im nächsten Dialog und klickt dann auf *OK*. Das Programm bietet euch ebenfalls an, starke Passwörter (über einen Zufallszahlengenerator) zu erstellen. Zusätzlich bietet KeyPassX, eine *Schlüsseldatei* auszuwählen, ohne die sich die Datenbank nicht verwenden lässt.

Um die Passwortdatenbank für die zukünftige Verwendung auf einem Datenträger zu speichern, klickt ihr auf *Datenbank* ► *Datenbank speichern*.

Methode II: Individuelle Gedächtnisstütze

Ihr merkt euch eine zufällig gewählte Seite eines euch bekannten Buches und denkt euch daraus eine *fiktive Schablone* aus, die verschiedene Buchstaben eines Satzes oder eine Abschnitts auf dieser Seite markiert. Verändert dann das so entstehende Wort durch das Einfügen von Ziffern und Sonderzeichen und das Anhängen weiterer Worte.

Ein praktisches Beispiel: Ich merke mir den Namen eines mir in Erinnerung bleibenden Buches und die Seite 373. Auf dieser Seite finde ich den Satz „*Er wollte sich mir nicht anvertrauen – und jetzt ist es zu spät.*“ Daraus bastle ich die Basis meines Passworts aus den Anfangsbuchstaben **Ewsmna-Ujiezs**. Dieses **Basis-Passwort** verwende ich nirgendwo. Ich nutze lediglich zwei *verschiedene Ableitungen* davon für unterschiedliche Zwecke. **Variante eins** (die Ziffern der Seitenzahl an ihrer jeweiligen Positionen eingefügt) für den Zugang zu meinem privaten pgp-key: **Ews3mna7-Uji3ezs** sowie **Variante zwei** (373 → §/§ auf einer deutschen Tastatur) für das Entschlüsseln meiner Festplatte: **Ew§/§smna-Ujiezs_against_the_empire**.

Dies ist u.a. vor dem Hintergrund der gesetzlich gedeckten Praxis zur Herausgabe von Passwörtern an Sicherheitsbehörden durch Diensteanbieter absolut notwendig!

Verwendet ein solches Basispasswort zum „Erzeugen“ weiterer Passwörter nur für die gleiche „Klasse“ von Passwörtern. Also Passwörter für *pgp, Datenträgerverschlüsselung* ***nicht mischen mit solchen für*** *ebay, amazon.*

Diese Methode hat jedoch den Nachteil, dass sich über die selbst ausgedachten Varianten des Basis-Passworts zwangsläufig menschliche „Muster“ einschleichen, die es eigentlich zu vermeiden gilt.

59 Ein *Keylogger* zeichnet jeden Tastenanschlag der Tastatur auf und kann somit auch eure Passwörter mitprotokollieren. Ein Keylogger kann eingeschleuste Schadsoftware oder aber auch ein nachträglich in die Tastatur oder am Verbindungskabel eingebauter Chip sein. Gegen letztere Varianten schützt Tails nicht!

Überschätzt euch nicht bei der Wahl eines zu komplexen Passworts. Gelingt euch die Rekonstruktion des Passwort über die Gedächtnisstütze nicht, bleiben die Daten für *euch* immer unzugänglich.

Es gibt keine 100%ige Sicherheit bei der Auswahl des *„richtigen" Passworts*. Und es wird, wie ihr in der Ergänzung im nächsten Abschnitt lesen könnt, noch komplizierter, wenn ihr den technischen Fortschritt mitzuberücksichtigen versucht. Letztendlich müsst ihr **zwischen Sicherheit und Nutzbarkeit abwägen** und selbständig entscheiden, was ihr euch zutraut und euren Bedürfnissen nach Sicherheit im Alltagsgebrauch am Nächsten kommt.

Hier nochmal kurz das Wichtigste zusammengefasst:

- Verwendet auf keinen Fall dieselben Passwörter für mehrere Zugänge. Also nicht für euer Mail-Postfach oder euer ebay-Konto dasselbe Passwort verwenden wie für den Zugang zu eurem Rechner.
- Hängt nicht einfach eine Zahlenkombination an ein existierendes Wort.
- Verwendet keine einfachen Buchstabenersetzungen wie m!s3r4b3| ← (MISERABEL).
- Auch keine einfache Zusammensetzung von (leicht veränderten) Wörtern.
- Entscheidet euch für eine der beiden Varianten: Merken oder verschlüsseltes Speichern eurer Passwörter. Notizen auf Zettel sind dabei eine sehr schlechte Alternative.
- Eine sogenannte **Passphrase** (komplexeres Passwort) für die Nutzung eures privaten *PGP-Schlüssel*, oder die Datenträgerverschlüsselung sollte tatsächlich länger und komplexer sein als ein (einfaches) Passwort für euren Mail-Account. Um auch zukünftig noch auf der sicheren Seite zu stehen, sollte sie mindestens 16 Zeichen lang sein.
- Wechselt eure Passwörter hin und wieder, insbesondere, wenn ihr den Verdacht habt, dass das Passwort bekannt geworden ist (z.B. durch einen Bedienfehler, copy&paste ins falsche Fenster, u.ä.).

DRITTENS: In Zukunft unsicher

Sich auf die Ebene der Analyse kryptografischer Methoden verschiedener Verschlüsselungsalgorithmen zu begeben, würde an dieser Stelle den Rahmen sprengen. Vereinfacht gesagt basiert die Sicherheit wichtiger aktueller Verschlüsselungsverfahren wie GPG auf mathematischen Problemen in Kombination mit sehr großen Zahlen. Während das Überprüfen, ob ein privater und ein öffentlicher Schlüssel zusammenpassen, kein Problem darstellt, ist das Auffinden eines zum öffentlichen Schlüssel passenden privaten Schlüssel eine extrem rechenintensive Aufgabe. Klassische Computer müssen schlicht alle möglichen Paare von Primfaktoren durchprobieren. Der Aufwand, eine solche Verschlüsselung mit klassischen Computern zu knacken, wächst exponentiell mit der Schlüssellänge. In Zahlen bedeutet dies, dass ein Angreifer bei einer Brute-Force-Attacke bei einer Schlüssellänge von 1024 Bit eine Anzahl von 2^1024-1 Zahlen nach Primzahlen durchsuchen und diese ausprobieren müsste, um den richtigen Schlüssel zu finden. Dies würde mit heutzutage zur Verfügung stehenden Rechenleistungen wahrscheinlich mehr als eine Lebensspanne dauern. Die Rechenleistung von Computerchips verbessert sich zur Zeit allerdings immer noch fortwährend aufgrund der weiter voran schreitenden Miniaturisierung der Schaltkreise und die Parallelisierung der Chips - zumindest solange, bis diese Entwicklung an ihre physikalischen Grenzen stoßen wird.

Quantencomputer

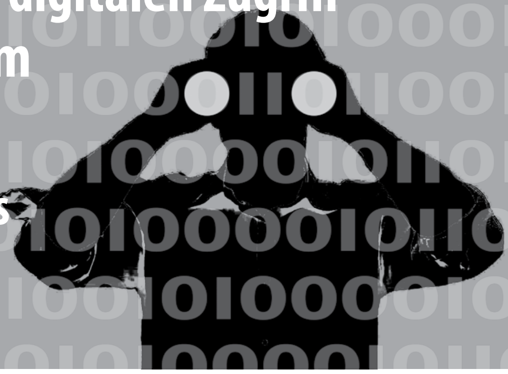
Vor über 20 Jahren entwickelte Peter Shor ein Quantenalgorithmus, dessen Rechenaufwand nicht exponentiell mit der Schlüssellänge wächst, sondern wesentlich kleiner ist. Allerdings ist die Umsetzung von leistungsstarken Quantencomputern mit hohen Kapazitäten und einer sicheren Vernetzung bislang aufgrund der äußerst schwierigen physikalischen Bedingungen noch nicht gelungen. Krypto-Expert*innen erwarten eine solche Realisierung auch nicht so bald. Trotzdem wird intensiv nach neuen Verschlüsselungsalgorithmen geforscht, die „quantenresistent" sind. Denn sollte eines Tages die Hardware für Quantencomputer mit ausreichend vielen Quantenbits entwickelt worden sein, dann wären asymmetrische Verschlüsselungsverfahren wie die, die GPG benutzt, nicht mehr sicher, unabhängig von der Schlüssellänge. Solange gilt jedoch: je langer der Schlüssellänge, umso sicher der Schlüssel vor Angreifer*innen.

Selbst jetzt ist es schon so, dass Schlüssellängen, die noch vor zehn Jahren als sicher galten, heute nicht mehr empfohlen werden. Diese technischen Entwicklungen können tatsächlich handfeste Konsequenzen für die Sicherheit wirklich sensibler Daten haben, die ihr z.B. auf einem verschlüsselten USB-Stick abgelegt habt. Sind diese Daten auch in fünf Jahren noch vor unerwünschtem Zugriff sicher? Stellt euch vor, jemand hat vor einiger Zeit eine Kopie eures verschlüsselten Datenträgers gemacht. Diese Daten wären dann trotz Verschlüsselung rückwirkend lesbar.

Es ist wichtig, sich zu überlegen, welche Daten trotz Verschlüsselung überhaupt auf der Festplatte, im Mailprogramm, auf dem Smartphone oder in einer Cloud gespeichert werden müssen. Im Zweifel ist sicheres Löschen die bessere Wahl!

Index

Hefte zur Förderung des Widerstands gegen den digitalen Zugriff
Band I: Tails - The amnesic incognito live system



Anleitung zur Nutzung des Tails-Live-Betriebssystems für sichere Kommunikation, Recherche, Bearbeitung und Veröffentlichung sensibler Dokumente

5. Auflage